PATIENT CONFIDENTIALITY

HEARING

BEFORE THE

SUBCOMMITTEE ON HEALTH

OF THE

COMMITTEE ON WAYS AND MEANS
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

MARCH 24, 1998

Serial 105–23

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE
49–195 CC WASHINGTON : 1998

COMMITTEE ON WAYS AND MEANS

BILL ARCHER, Texas, *Chairman*

PHILIP M. CRANE, Illinois
BILL THOMAS, California
E. CLAY SHAW, JR., Florida
NANCY L. JOHNSON, Connecticut
JIM BUNNING, Kentucky
AMO HOUGHTON, New York
WALLY HERGER, California
JIM MCCRERY, Louisiana
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
JIM NUSSLE, Iowa
SAM JOHNSON, Texas
JENNIFER DUNN, Washington
MAC COLLINS, Georgia
ROB PORTMAN, Ohio
PHILIP S. ENGLISH, Pennsylvania
JOHN ENSIGN, Nevada
JON CHRISTENSEN, Nebraska
WES WATKINS, Oklahoma
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY HULSHOF, Missouri

CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
ROBERT T. MATSUI, California
BARBARA B. KENNELLY, Connecticut
WILLIAM J. COYNE, Pennsylvania
SANDER M. LEVIN, Michigan
BENJAMIN L. CARDIN, Maryland
JIM MCDERMOTT, Washington
GERALD D. KLECZKA, Wisconsin
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
WILLIAM J. JEFFERSON, Louisiana
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
KAREN L. THURMAN, Florida

A.L. SINGLETON, *Chief of Staff*
JANICE MAYS, *Minority Chief Counsel*

SUBCOMMITTEE ON HEALTH

BILL THOMAS, California, *Chairman*

NANCY L. JOHNSON, Connecticut
JIM MCCRERY, Louisiana
JOHN ENSIGN, Nevada
JON CHRISTENSEN, Nebraska
PHILIP M. CRANE, Illinois
AMO HOUGHTON, New York
SAM JOHNSON, Texas

FORTNEY PETE STARK, California
BENJAMIN L. CARDIN, Maryland
GERALD D. KLECZKA, Wisconsin
JOHN LEWIS, Georgia
XAVIER BECERRA, California

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

Page

Advisory of March 17, 1998, announcing the hearing 2

WITNESSES

American Medical Management, Jim Sloane 45
Borowitz, Stephen M., M.D., University of Virginia Health Sciences Center 28
Goldman, Janlori, Georgetown University 34
MacGregor Medical Association, James Birge, M.D., and Jim Sloane, American Medical Management 45
Mayo Clinic, Sherine E. Gabriel, M.D 59
Merck Research Laboratories, and Merck & Co., Inc., Harry A. Guess, M.D 64
U.S. National Committee on Vital and Health Statistics, Don E. Detmer, M.D 6

SUBMISSIONS FOR THE RECORD

American Association of Health Plans, statement 77
American Association of Occupational Health Nurses, statement 84
American College of Occupational and Environmental Medicine, Arlington Heights, IL, statement 90
American Hospital Association, statement 91
Avorn, Jerome L., M.D., and Elizabeth Andrews, International Society for Pharmacoepidemiology, letter and attachments 97
Frantz, Rita, National Pressure Ulcer Advisory Panel, Alexandria, VA, statement 103
Healthcare Leadership Council, statement 94
International Society for Pharmacoepidemiology, Jerome L. Avorn, M.D., and Elizabeth Andrews, letter and attachments 97
Medical Group Management Association, statement 99
National Breast Cancer Coalition, statement 101
National Pressure Ulcer Advisory Panel, Alexandria, VA, Rita Frantz, statement 103
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, statement 106

PATIENT CONFIDENTIALITY

TUESDAY, MARCH 24, 1998

HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON HEALTH,
Washington, DC.

The Subcommittee met, pursuant to call, at 10 a.m., in room 1100, Longworth House Office Building, Hon. Bill Thomas (Chairman of the Subcommittee) presiding.

[The advisory announcing the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON HEALTH

FOR IMMEDIATE RELEASE
March 17, 1998
No. HL–20

CONTACT: (202) 225–3943

Thomas Announces Hearing on Patient Confidentiality

Congressman Bill Thomas (R–CA), Chairman, Subcommittee on Health of the Committee on Ways and Means, today announced that the Subcommittee will hold a hearing on patient confidentiality. The hearing will take place on Tuesday, March 24, 1998, in the main Committee hearing room, 1100 Longworth House Office Building, beginning at 10:00 a.m.

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

BACKGROUND:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of Health and Human Services to submit to the Congress "detailed recommendations with respect to the privacy of individually identifiable health information." In developing her recommendations, the Secretary was required to consult with the National Committee on Vital and Health Statistics and the Attorney General. The Secretary released her report on September 11, 1997, and Congress has until August 1999 to pass legislation to protect individual patient confidentiality. If the Congress does not enact legislation, HIPAA directs the Secretary to issue her own final enforceable regulations by February 2000.

Health care information is used for a variety of purposes including research, disease prevention, quality assurance, and outcomes measurements. In recent years, health care information has moved away from paper records to electronic records. This innovation provides tremendous opportunities for medical advances as well as new challenges for maintaining patient confidentiality. The Administration's recent announcement of a delay in the implementation of the HIPAA administrative simplification provisions underscores the complexity of maintaining confidentiality in an information age.

In announcing the hearing, Chairman Thomas stated: "Our nation has a great history of leadership in medical advances and health care innovation. I have seen, first hand, examples of health care data being used to help in the discovery of new medical techniques and technologies. In addition, outcomes studies and consumer information based on up-to-date health care data can make our nation's health care system better, services more readily available, and care more affordable. However, it is essential that patient confidentiality concerns are addressed while maintaining access to data to promote better health."

FOCUS OF THE HEARING:

The hearing will focus on patient confidentiality from the perspective of the health care consumers, physicians, providers, and researchers.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Any person or organization wishing to submit a written statement for the printed record of the hearing should submit at least six (6) single-space legal-size copies of their statement, along with an IBM compatible 3.5-inch diskette in ASCII DOS Text or WordPerfect 5.1 format only, with their name, address, and hearing date noted on a label, by the close of business, Tuesday, April 7, 1998 , to A.L. Singleton, Chief of Staff, Committee on Ways and Means, U.S. House of Representatives, 1102 Longworth House Office Building, Washington, D.C. 20515. If those filing written statements wish to have their statements distributed to the press and interested public at the hearing, they may deliver 200 additional copies for this purpose to the Subcommittee on Health office, room 1136 Longworth House Office Building, at least one hour before the hearing begins.

FORMATTING REQUIREMENTS:

Each statement presented for printing to the Committee by a witness, any written statement or exhibit submitted for the printed record or any written comments in response to a request for written comments must conform to the guidelines listed below. Any statement or exhibit not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All statements and any accompanying exhibits for printing must be typed in single space on legal-size paper and may not exceed a total of 10 pages including attachments. At the same time written statements are submitted to the Committee, witnesses are now requested to submit their statements on an IBM compatible 3.5-inch diskette in ASCII DOS Text or WordPerfect 5.1 format. Witnesses are advised that the Committee will rely on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. A witness appearing at a public hearing, or submitting a statement for the record of a public hearing, or submitting written comments in response to a published request for comments by the Committee, must include on his statement or submission a list of all clients, persons, or organizations on whose behalf the witness appears.

4. A supplemental sheet must accompany each statement listing the name, full address, a telephone number where the witness or the designated representative may be reached and a topical outline or summary of the comments and recommendations in the full statement. This supplemental sheet will not be included in the printed record.

The above restrictions and limitations apply only to material being submitted for printing. Statements and exhibits or supplementary material submitted solely for distribution to the Members, the press and the public during the course of a public hearing may be submitted in other forms.

Note: All Committee advisories and news releases are available on the World Wide Web at 'HTTP://WWW.HOUSE.GOV/WAYS__MEANS/'.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202–225–1721 or 202–226–3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Chairman THOMAS. The Subcommittee will come to order.

Each day, millions of Americans receive medical treatment. Increasingly, patients receive their care from a multifaceted system of health care entities and professionals. As our health care system

has evolved from a solo practitioner to complex integrated health systems and everything in between, so has the challenge of ensuring that patients' private information is not improperly disclosed and used for inappropriate purposes.

National attention regarding the confidentiality of patient information was heightened with the passage of the Health Insurance Portability and Accountability Act of 1996. This act required the Secretary of Health and Human Services to consult with the National Committee on Vital and Health Statistics and the Attorney General and to report to the Congress her "detailed recommendations with respect to the privacy of individually identifiable health information." The Secretary released a report on September 11, 1997. Congress now has until August 1999 to pass legislation to protect that individual patient confidentiality. Without legislation, the law says the Secretary will write her own regulations.

Today this Subcommittee begins its exploration of this important topic. We will hear from experts representing various parts of the health care system who will share with us their views regarding the confidentiality of patient information. In reading their testimony, it was clear to me we are dealing with a very important but very delicate issue. If the Congress errs on the side of overprotection, we could stifle medical innovation and research which would adversely impact public health. Likewise, if we fail to provide the American public with adequate reassurance that their individually identifiable information is protected, some may avoid, delay, or carry out protective behavioral patterns dealing with necessary treatments.

Time is critical, not just because the Secretary will issue her own regulations in August 1999 if Congress does not act, but as we will hear on one of our panels today, if Congress does not act, States are already acting. And we run the chance, if we do not provide at least guidance if not some uniformity, of a crazy quilt pattern confronting us in which no one's wishes are granted, and that is a very real possibility.

[The opening statement follows:]

Opening Statement of Chairman Bill Thomas

Each day, millions of Americans receive medical treatment. Increasingly, patients receive their care from a multi-faceted system of health care entities and professionals. As our health care system has evolved—from the solo practitioner to complex integrated health systems—so has the challenge of ensuring that patients' private information is not improperly disclosed and used for inappropriate purposes.

National attention regarding the confidentiality of patient information was heightened with the passage of the Health Insurance Portability and Accountability Act of 1996. This Act required the Secretary of Health and Human Services to consult with the National Committee on Vital and Health Statistics and the Attorney General and to report to the Congress her "detailed recommendations with respect to the privacy of individually identifiable health information." The Secretary released her report on September 11, 1997. The Congress now has until August 1999 to pass legislation to protect individual patient confidentiality. Without legislation, the Secretary will write her own regulations.

Today, this Subcommittee begins its exploration of this important topic. We will hear from several experts, representing various parts of the health care system, who will share with us their views regarding the confidentiality of patient information. In reading their testimony, it was clear to me that we are dealing with a very delicate issue. If the Congress errs on the side of over-protection, we could stifle medical innovation and research which would adversely impact public health. Likewise, if we fail to provide the American public with adequate reassurance that their individ-

ually identifiable information is protected, some may avoid or delay necessary treatments.

I look forward to hearing from our first witness, Dr. Don Detmer, Chair of the National Committee on Vital and Health Statistics.

Chairman THOMAS. I look forward to hearing from all of our witnesses, but our first witness, Dr. Don Detmer, is the chair of the National Committee on Vital and Health Statistics. And Dr. Detmer, before I recognize you, I would ask my colleague from Wisconsin if he has any opening statement. Or if he has a written statement from the Ranking Member, I would make that a part of the record. But I would recognize the gentleman from Wisconsin.

Mr. KLECZKA. Mr. Chairman, I do not know if Mr. Stark has an opening statement, but if he does, I would ask that that be included. I would also like to introduce into the record a statement from myself on this timely issue.

I want to acknowledge the Chairman's interest in the subject matter, although when he talks about overprotection, I don't think we are anywhere near that problem when it comes to a patient's records. In fact, just a short time ago in the local papers, I think two or three local drugstores were involved in selling their patient lists to drug companies. In response to that, consumers received mailings from drug companies.

I think privacy concerns are something we should be taking more seriously in this Congress, not only as it deals with the Internet and Social Security numbers, but now we have seen in the most recent past a series of drugstores selling their patient lists. I think Congress should not sit idly by while all this continues to happen. I think we should be proactive and err on the side of the consumer.

Thank you, Mr. Chairman.

[The opening statement follows:]

Opening Statement of Congressman Jerry Kleczka

I am pleased Chairwoman Thomas has called this hearing on medical privacy today. This public debate will draw attention to one of the most important issues facing the subcommittee and American public: guaranteeing the privacy of all Americans' personal and medical information. This guarantee is particularly important given the rapid technological advances and awe-inspiring medical discoveries being made every day.

I was appalled, as I am sure many of my colleagues were, to read in recent Washington Post articles about drugstores selling confidential patientprescription information to outside companies for marketing purposes. While the companies in question quickly changed their practices when consumers expressed outrage at these revelations, the practice of selling prescription information to third parties continues to go on throughout the nation.

Imagine simply going to the local drug store to fill a prescription, and, without your permission, the pharmacist behind the counter transmits your medical and prescription information to a direct marketing firm. Certainly, innocent consumers filling prescriptions should have at the very least an expectation of privacy. Sending confidential prescription information to a marketing company that has absolutely no medical expertise or purpose for receiving that information other than to profit from it raises serious ethical questions. I believe legitimate checks can and should be placed on this type of practice.

Too many Americans operate under the assumption that their private medical records are just that, private. However, in today's computer age where personal information can be transmitted across the country quite literally at a push of a button, threats to the privacy of individuals' medical records have never been greater. While this technological innovation has provided opportunities for and lead to im-

portant medical advances, it has come with price—the price of sacrificing one's personal privacy and security.

There are, of course, appropriate uses for electronically transmitting medical information. For example, managed care networks, insurers, medical researchers, or benefits managers arguably have legitimate needs for quick and easy access to medical records. However, the idea that potentially thousands of individuals could gain access to this electronic data—something so sacred and private as a diagnosis of mental illness or terminal illness, for example—gives me pause. I find it even more troubling that this private information can and is electronically transmitted for absolutely no legitimate medical purpose. Transmitting this information to a third-party solely to improve the profit margins of a pharmaceutical company is simply unconscionable.

The Health Insurance Portability and Accountability Act of 1996 required the Secretary of Health and Human Services to submit detailed recommendations with respect to the privacy of individual's health information. The Secretary released her report this past September and we in Congress have until August 1999 to pass legislation protecting patient confidentiality. My hope is that as we prepare this legislation Congress will not only reflect back on the testimony heard today, but also on the missteps and breaches of confidentiality that have occurred in the past and place strong protections for the future.

Chairman THOMAS. I thank the gentleman. Our goal is not to err on either side but to pass informed legislation. Our goal is not to legislate by anecdote but be informed legislators. That is the purpose of this hearing.

And with that, I recognize Dr. Detmer and tell him that the written statement he has will be made a part of the written record, without objection, and you can address us in any way you see fit in the time you have available.

Dr. DETMER. Thank you very much, Mr. Chairman. Good morning.

Chairman THOMAS. I will tell you in advance these microphones are unidirectional and you have to speak directly into them and relatively close.

STATEMENT OF DON E. DETMER, M.D., CHAIRMAN, U.S. NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS

Dr. DETMER. I appreciate the opportunity to appear before the Subcommittee on this extraordinarily important legislative issue. Privacy, confidentiality, and security of individual health information touches the lives of all Americans in a very personal way, and your actions will influence the future course of health care and the future of medicine itself.

I am a university professor and senior vice president at the University of Virginia and a practicing surgeon. I am here today in my role as chair of the National Committee on Vital and Health Statistics. As you are aware, the committee is a nearly 50-year-old statutory public advisory body to the Secretary of Health and Human Services on health data privacy and health information policy. Its 18 members include four practicing physicians.

Through the mandates of the 1996 Health Insurance Portability and Accountability Act, the committee's responsibilities were broadened to encompass health statistics, privacy, and computer-based clinical records for both the public and private sector. Last June the committee provided its initial recommendations to the Sec-

retary and she, in turn, submitted her detailed recommendations to Congress last September.

All in all, the committee held over 20 days, full days, of public hearings and heard from more than 200 witnesses who discussed data standards, privacy, and security issues. The hearings included representatives from across the entire spectrum of the health community. This extensive public consultation was immensely helpful to us as we formulated our recommendations to Secretary Shalala, and we continue to hold hearings to further refine our advice.

Our hearings showed strong and widespread support for Federal health privacy legislation. At the same time, it is clear our society has not yet reached a consensus about the definition and boundaries of privacy in an information age. The committee has concluded that our Nation faces a privacy crisis today, and legislation is urgently needed to address two policy deficiencies.

First, we lack solid Federal legislation on fair information practices for personal health information. Second, we lack sufficient antidiscrimination statutes to keep personal health information from being used against citizens in areas such as employment and insurability. With the fast pace of progress in medicine and technology, this further complicates an already complex situation.

With the exception of one abstention, all the recommendations from the Committee were unanimous. What does the committee wish to see in this legislation?

We want a law that requires creators and users of identifiable health information to ensure a full range of fair information practices, including the patient's right of access to his or her records, the right to seek amendment of records, and the right to be informed about users and uses of health information.

We seek reasonable restrictions and conditions on access to and use of personally identifiable health information that maintains protections for the information as it passes into the hands of secondary and tertiary users, so that there are no loopholes that allow information to escape appropriate controls.

We seek adequate security for health data, no matter what media are used to create, transmit, or store data. That is, we wish the protections to apply to the data itself and not to whatever medium or technology is used.

We want those who create and use personally specific health information to accept accountability for actions that affect privacy interests of patients. We support sanctions when restrictions are violated.

We wish to promote the use of nonidentifiable, coded, or encrypted information when a function can be fully and substantially accomplished without more specific identifiers.

The committee strongly supports the use of health records for all forms of legitimate health research without a case-by-case patient consent for access to such data, subject to independent review of research protocols and other procedural protections for patients.

The committee also strongly supports the use of health records for public health purposes, subject to substantive and procedural barriers commensurate with the importance of public health function.

The committee believes patients need strong substantive and procedural protections if their records are to be disclosed to law enforcement officials.

The committee strongly supports limiting use and disclosure of identifiable information to the minimum amount necessary to accomplish the purpose. The committee also strongly believes when identifiable health information is made available for nonhealth uses, patients deserve a strong assurance that the data will not be used to harm them.

We urge the Congress to pass such legislation during this session, since we do not believe the HIPAA privacy regulatory authority is an adequate alternative to legislation.

Clearly, with the continued development of computer-based patient health records, it would be best to integrate the appropriate security and policy procedures into the emerging architecture of such systems, and this will require action now rather than later since these systems are being built as I speak to you. Action now should allow us to avoid a variant of the "year 2000" problem in this age of computers.

The committee recognizes drafting and passage of the health privacy law will not be easy. Health privacy legislation presents hard choices and difficult tradeoffs. Health records are primarily used for the treatment of patients, to improve the quality of care, reduce the cost of health care, expand the availability of health care, protect the public health, and assure public accountability of the health care system. Privacy competes with all of these objectives, and it will not be easy to strike a widely accepted balance between privacy and these other worthy goals. The new legislation must reflect the current structure and legislative framework for health care and allow for continued progress in health care.

In summary, two sets of legislation are needed. The first involves the relationship between privacy as defined by principles of fair information practices; and the second relates to concerns about discrimination based on health status or conditions. The antidiscrimination provisions of HIPAA need to be expanded to cover all aspects.

Whether or not general privacy concerns and discrimination concerns should be addressed together in the same piece of legislation, you can best decide. An already complex health privacy accountability bill may not be the best place to sort out responses to the important discrimination problems.

The National Committee on Vital and Health Statistics calls on everyone to work together in good faith. Everyone should benefit from a well-crafted set of fair information practices for health information. Patients will have new rights and greater protections for sensitive information. Critically important, trust in the provider-patient relationship will be preserved. Providers and insurers will have clearer rules and responsibilities. Secondary users will know when they can and cannot have information and what their obligations and penalties are if these obligations are ignored.

The committee is pleased to provide a public forum for continued advice on these issues, and we look forward to working with you and others to achieve a comprehensive and balanced public privacy health information law.

Thank you, Mr. Chairman. I would be happy to answer questions.

[The prepared statement follows:]

Statement of Don E. Detmer, M.D., Chairman, U.S. National Committee on Vital and Health Statistics

INTRODUCTION

Thank you, Mr. Chairman. It is a pleasure to appear before the Committee today to discuss health information privacy, confidentiality, and security issues. I am currently University Professor and Senior Vice President at the University of Virginia and a practicing surgeon. I appear before you today in my role as chair of the National Committee on Vital and Health Statistics (NCVHS). The NCVHS is the statutory public advisory body to the Secretary of Health and Human Services on health data, privacy and national health information policy.

The NCVHS has a distinguished, nearly fifty year history of providing the government with broad based advice on health data issues, including data needed to assure the quality of care, meet public health needs as well as data needs for other purposes. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) assigned the committee new responsibilities for health information policy development on data standards, privacy, and computer-based clinical records for both the public and private sectors.

The Committee is made up of 18 members, sixteen appointed by the HHS Secretary, one appointed by the Speaker of the House and one appointed by the President *pro tempore* of the Senate. Members are appointed from among individuals who have distinguished themselves in a variety of fields ranging from privacy and security of health information to the provision of health services and population-based public health. Four of the current members are practicing physicians.

As a result of the passage of HIPAA, the nation has the potential to achieve major improvements in the quality and effectiveness of health care and the efficiency of the health sector through improved information technology. And the law provides this opportunity in a national framework that protects the privacy and security of health information. The primary focus of the law is on private health insurance reform. However, the provisions on Administrative Simplification outline a new national framework for health data standards, security and health information privacy in the U.S.

Today, I will focus on the health information privacy provisions of HIPAA, and especially on the NCVHS's recommendations to HHS relating to health information privacy. HIPAA required that the Secretary of Health and Human Services submit "detailed recommendations" to the Congress "with respect to the privacy of individually identifiable health information." In preparing her recommendations, the Secretary was directed to consult with the National Committee on Vital and Health Statistics. Last June, the NCVHS provided our initial recommendations on privacy, confidentiality, and security to Secretary Shalala. She, in turn, submitted her detailed recommendations to Congress last September.

Our full report is available on the NCVHS website: http://aspe.os.dhhs.gov/ncvhs, and the Secretary's privacy recommendations are available on the HHS administrative simplification website: http://aspe.os.dhhs.gov.admnsimp.

NCVHS HEALTH INFORMATION PRIVACY RECOMMENDATIONS

As a basis for our privacy recommendations, the NCVHS held six full days of public hearings last year during which we heard from over 40 witnesses. All in all, we held over 20 full days of public hearings and heard from more than 200 witnesses who discussed data standards, privacy and security issues. The hearings included representatives from across the entire spectrum of the health community, including the privacy community, research, public health, quality assurance, insurance, managed care, law enforcement and oversight, providers, claims processors, the drug industry, federal agencies and consumer interest groups. This public consultation was immensely helpful to us as we formulated our recommendations to Secretary Shalala.

First of all, our hearings showed strong and widespread support for federal health privacy legislation. And with the exception of one abstention, all recommendations of the committee were unanimous. The committee had difficulty with the definition of privacy as it relates to the confidentiality and security of person-specific health information. It chose to use the word "privacy" in its report mainly since the word

has been the major term used in public discussion of this topic. The culture has yet to reach a consensus on what privacy should mean in contemporary society.

Be that as it may, the committee concluded that the United States is in the midst of a health privacy crisis. The protection of health records has eroded significantly in the last two decades. Major contributing factors are ongoing institutional changes in the structure of the health care system and the lack of modern privacy legislation. Without a federal health privacy law, patient protections will continue to deteriorate in the future.

We also concluded that the importance of trust in the provider-patient relationship must be preserved. Patients must feel comfortable in communicating sensitive personal information. Delays in passing privacy legislation will allow additional and uncontrolled uses of health information to develop. Failure to address health data privacy concerns can undermine public confidence in the health care system, expose patients to continuing invasions of privacy, subject record keepers to potentially significant legal liability, and interfere with the ability of health care providers and others to operate the health care delivery and payment system in an effective and efficient manner.

The greater the delay in imposing meaningful controls on inappropriate use and disclosure of identifiable health information, the more difficult it may be to generate enthusiasm for instituting necessary restrictions on use and disclosure, or change the way that information is acquired, maintained, and used. Clearly, with the continued development of computer-based patient record systems, it would be best to integrate the appropriate security and policy procedures into the emerging architecture of such systems.

The NCVHS recommended that the Secretary and the Administration assign the highest priority to the development of a strong position on health privacy that provides the highest possible level of protection for the privacy rights of patients. Any realistic proposal must properly balance the important and well-established interests of patients in the protection of their health information and the legitimate needs of the health care system to provide and pay for health care in an efficient, effective and fair manner while supporting the responsible use of health records for public health and health research, and other legitimate social purposes.

The Health Insurance Portability and Accountability Act provides that if the Congress does not pass privacy legislation by August 1999, then the Secretary of HHS is authorized to issue regulations containing standards for the privacy of electronic administrative and financial transactions. However, the Committee found a clear and strong preference for a comprehensive legislative solution, rather than addressing health privacy through the regulatory process alone.

It is difficult to address health privacy requirements in a piecemeal fashion. Rules that only cover electronic health care transactions but not paper-based transactions or other types of health records could prove very difficult to develop or administer. Further, the committee firmly believes that policy on data confidentiality and security should not be contingent upon the form, medium, or technology used to record or work with health data, e.g., paper, fax, or an electronic medium.

Consequently, the NCVHS strongly recommends that the Congress enact a health privacy law before it adjourns this fall. Leaders in both House and Senate should publicly endorse the need for strong and effective privacy legislation that provides meaningful protections to patients. Congressional leaders should ask relevant legislative committees to agree to a timetable for action. The Congress should not treat the existence of the regulatory authority as an adequate alternative to legislation.

The Committee calls for a law that requires creators and users of identifiable health information to——

- ensure a full range of fair information practices, including a patient's right of access to records, right to seek amendment of records, and right to be informed about uses of health information;
- accept reasonable restrictions and conditions on access to and use of identifiable health information;
- maintain protections for health information as it passes into the hands of secondary and tertiary users so that there are no loopholes that allow health information to escape from privacy controls;
- provide adequate security for health data no matter what media are used to create, transmit, or store data;
- accept accountability for actions that affect the privacy interests of patients;
- promote the use of non-identifiable, coded, or encrypted information when a function can be fully or substantially accomplished without more specific identifiers.

The law must also impose restrictions on disclosure and use of the information and impose sanctions for violations.

The Committee strongly supports the use of health records for health research without a case by case patient consent for access to such data, subject to independent review of research protocols and other procedural protections for patients.

The Committee also strongly supports the use of health records for public health purposes, subject to substantive and procedural barriers commensurate with the importance of the public health functions.

The Committee believes that patients need strong substantive and procedural protections if their health records are to be disclosed to law enforcement officials.

The Committee strongly supports limiting use and disclosure of identifiable information to the minimum amount necessary to accomplish the purpose. The Committee also strongly believes that when identifiable health information is made available for non-health uses, patients deserve a strong assurance that the data will not be used to harm them.

The Committee recognizes that the drafting and passage of a health privacy law will not be easy. Health privacy legislation presents hard choices and difficult tradeoffs. Health records are primarily used for the treatment of patients and to improve the quality of health care, reduce the costs of health care, expand the availability of health care, protect the public health, and assure public accountability of the health care system. Privacy competes with all of these objectives, and it will not be easy to strike a widely accepted balance between privacy and these other worthy goals. As mentioned earlier, the task is not made any easier by the lack of agreement about what privacy even means in contemporary American society.

In our hearings, users of health information uniformly expressed strong support for privacy legislation. However, most users also asked that no—or at most few—new restrictions be placed on their ability to collect, use, and disclose health information. The Committee believes that it is unfair and unreasonable for any health data user to expect that health privacy legislation will not require some change in policy and practice. Everyone—patients and record keepers alike—will benefit from health privacy legislation, and everyone is likely to pay some price for the legislation.

At the same time, the Committee recognizes that privacy legislation must take into account the complexity and the needs of the current health care delivery and payment system. New legislation must reflect the current structure and legislative framework for health care. Changes can and must be made, but no one can expect that the health care system will be restructured solely in the interests of privacy and without regard to cost. Indeed, achieving cost savings from administrative simplification was a key driver behind the Health Insurance Portability and Accountability Act of 1996. The Committee has no doubt that a privacy bill can be passed that balances the interests of patients with the needs of the health care system.

The Committee also recognizes that passing legislation will not end either the debate or the struggle to accomplish desired improvements. Once a law passes, record keepers will have to change to accommodate the new rules, federal and state agencies will have to oversee implementation of the new law, and the Congress may be called upon to refine the law in the future. International data protection standards are being developed, and the United States needs to be a full partner in this effort.

Special Issues

Let me now turn to several additional issues that we heard about in our hearings.

Need for Anti-Discrimination Law

One issue that arose from time to time during the hearings was the relationship between privacy (as defined by principles of fair information practices) and discrimination. Clearly some motivation for protecting health information is to prevent the discriminatory use of the information both inside and outside the health care setting. Patients receiving care for some health conditions or who have been the subject of genetic testing have been and continue to be the subject of discrimination in employment, insurance, and elsewhere. Several current bills address the possible discriminatory use of genetic information.

Discrimination based on health status and condition remains a major and important concern, and it deserves a legislative solution. Whether or not general privacy concerns and discrimination concerns should be addressed together in the same piece of legislation, you can best decide. However, an already complex health privacy and confidentiality bill may not the best place to sort out responses to equally complex discrimination problems. The Committee suggests that privacy and discrimination issues both deserve explicit legislative treatment. The Committee urges the Congress to consider legislation expanding the anti-discrimination provisions of HIPAA to cover all aspects of discrimination based on health status and condition.

Preemption

Perhaps the most difficult conflict identified during our hearings is over preemption of state laws. Among large segments of the health industry, a major benefit to federal legislation is a high degree of regulatory uniformity throughout the country. The interstate nature of health care treatment and payment activities is readily apparent. By one estimate, approximately half of the U.S. population lives near the border of another state. To have a patient work in the District of Columbia, reside in Maryland, and receive care in Virginia creates a nightmare for the health care system to track unless substantial uniformity of policies and procedures exists. It will be difficult for many involved in electronic transfers of health data to accept any proposal that does not offer significant relief from the prospect of 50 different state laws establishing separate rules.

On the other hand, it would be difficult for many patient groups, privacy advocates and perhaps some provider groups to accept any proposal that does not allow states to adopt stronger privacy protections as specified in the HIPAA. People disagree whether existing state laws offer greater protection than most of the current federal proposals. There is strong support in some communities for a solid federal confidentiality standard that allows states to erect stronger privacy barriers. This was the approach that Secretary Shalala recommended last September.

The Committee suggests, however, that this issue need not be treated as a single problem with a single solution. The conflicts need to be broken down into components, and each component analyzed separately. In some areas, the case for federal preemption may be strong. For example, it may be unnecessarily complex to support 50 different patient access procedures. On the other hand, the need to recognize the diversity of state public health laws is already clearly reflected in most proposals. No one has suggested or is likely to support a uniform federal public health law. A narrower and careful analysis of preemption may help to minimize the admittedly strong conflicts here and may point to more effective resolutions. However, if sufficient national conformity is not achieved, both national and international objectives cannot be met.

The Committee stands willing to respond to such remaining issues in new legislation if and as the Congress desires.

Unique Health Identifier for Individuals

Because of privacy concerns, the NCVHS has recommended that HHS not adopt a standard for unique identifier for individuals as called for in HIPAA until privacy legislation is enacted. The NCVHS stated that "...it would be unwise and premature to proceed to select and implement such an identifier in the absence of legislation to assure the confidentiality of individually identifiable health information and to preserve an individual's right to privacy."

The NCVHS outlined three sets of concerns. First, we noted that the selection of a unique health identifier for individuals will become the focus of tremendous public attention and interest, far beyond that afforded to other health privacy decisions. No choice, the Committee concluded, should be made without more public notice, hearings and comment.

Second, we concluded that, until a new federal law adequately protects the confidentiality of the health record, it is not possible to make a sufficiently informed choice about an identification number or procedure. The degree of formal legal protection in such a law will have a major influence on both the decision itself and the public acceptance of that decision. Indeed, we would hope that passage of a comprehensive health privacy law would make the choice of an identifier easier, e.g., less threatening.

Finally, the NCVHS stated that a unique health identifier could not be protected from misuses under current law, notwithstanding the criminal penalties for wrongful disclosure enacted in HIPAA.

At the same time, the Committee feels an obligation to address the law and provide advice on this controversial matter. Accordingly, we are planning to hold several public hearings around the country to gather information and explore the issue further. This will be done in conjunction with the planned publication by HHS of a Notice of Intent to gather descriptive and evaluative information on unique identifiers for use in the health system on a systematic basis, including current practices, before developing any further recommendations. Lack of unanimity from the committee on this topic may occur, reflecting the difficult nature of the problem.

Computer Technology

Testimony received by the Committee showed that computers are perceived differently by different individuals and groups. Some view them as major threats to

patient privacy and others as tools for offering far greater protection of personal health data than is achievable with paper records. In terms of limiting release to selected information, computer-based data offers the greatest potential to avoid revealing patient identifiers. Others see computerized repositories of health data as magnets for hackers and other abusers and presume huge health data repositories are forthcoming. Testimony suggested that the real threats to computerized information—as with paper records—come from insiders and not from hackers. Unfortunately, this debate is hampered by a lack of sufficient, good health services research on the frequency and seriousness of problems in this area. Anecdotal information abounds with legitimate questions remaining as to its validity and representativeness.

Some have suggested that the patient authorization process should be expanded and that patients should be asked or permitted to make decisions about whether their information may or may not be computerized. The Committee is not sympathetic to the notion that patients should have a choice in the technology used to create, store and transmit health information. This is not a choice that record subjects for records maintained by other third party record keepers such as banks and employers. Requiring health record keepers—who are spending vast sums on computerization—to retain parallel paper systems is impractical and costly. It would deny the benefits and savings that the Congress has already determined will result from increased use of modern information technology.

Computers are an inevitable part of modern health care and indeed are intrinsic to the actual delivery of hospital care today. In addition, computer technology can provide strengthened confidentiality protections for personal health information. We should move on to debate the proper protections for records in a computerized environment. One response would be increased criminal and civil penalties for misuse of computerized health records. These penalties should apply to both inside and outside abusers of health data.

Law Enforcement

Testimony revealed sharp differences over the standards and procedures that should govern law enforcement access to health records. The law enforcement community contends that its track record accessing health records is a good one and that its access authority is not abused. Some health care providers and privacy advocates, however, seek to establish higher standards that would require law enforcement requests for records to obtain court orders, to provide patient notice, and to expressly justify each access to records.

Several privacy proposals would prevent use of health records against the record subject if an investigation of a provider brought to light criminal activity by the patient other than health care fraud.

This is the one major one area where the NCVHS respectfully differs from Secretary Shalala's recommendations. She recommended no changes to existing laws relating to law enforcement access to personal health information. Striking a balance between the needs of law enforcement and the privacy interests of patients is difficult but a crucial piece of this entire puzzle.

The Committee believes that patients need strong substantive and procedural protections if their health records are to be disclosed to law enforcement officials. Investigators should be required to justify the need for patient identifiers and to remove identifiers at the earliest possible opportunity. Other HIPAA provisions restrict the use of health information against the subject of the record unless the investigation arises out of and is directly related to health care fraud. If law enforcement wants to use the record in another way, it must first obtain a court order. That is one procedural barrier that is also included in several current privacy legislative proposals. Other proposals go further by requiring notice to the patient in some cases.

CONCLUSION

The NCVHS calls on everyone to work together in good faith. It is crucial that the Congress pass a balanced law as quickly as possible. Each year, health information becomes available for new uses, often without any legal, administrative, or policy barriers. Unless legislation passes soon, the risks to both patients and record keepers grow.

Everyone should benefit from a well-crafted set of fair information practices for health information. Patients will have new rights and greater protections for sensitive information. Providers and insurers will have clearer responsibilities and rules. Secondary users will know when they can have health information, when they cannot, what their obligations are, and what penalties will result if these obligations

are ignored. None of these benefits will be achieved unless everyone approaches the legislative process with a spirit of compromise.

The NCVHS is pleased to provide a public forum for deliberation and advice on these issues, and we look forward to working with HHS, the Executive Branch and the Congress on a comprehensive and balanced health information privacy law.

Thank you, Mr Chairman. I would be happy to answer any questions.

Chairman THOMAS. Thank you very much, Doctor. I guess the easiest way to start would be to indicate that in your testimony you said that Congress should not treat the existence of the regulatory authority as an adequate alternative to legislation.

Would you expand on that? Do you have any particular concerns about the Department of Health and Human Service's ability to promulgate such regulations? Or is it just too important to leave up to an agency, and Congress' responsibility ought to be to grapple with this question? What is it that worries you about letting the process go the way the legislation is structured?

Dr. DETMER. The key limitation of the process is that the law, as written, covers electronic and computer-based information and not paper and other forms, and that is the principal concern. So, essentially, the legislation really has a more limited scope.

The committee also feels the legislation dealing with this more broadly can generally craft a better response.

Chairman THOMAS. I have been impressed with the learning curve of a number of individuals who have been almost outspoken, I guess, advocates for privacy, and their understanding of that. Electronic data can, if done properly, be even better protected than paper records.

Do you believe there is any role currently or in the near future for a rather directed movement toward electronic rather than the keeping of paper records; either carrots or sticks of some sort to move more rapidly into electronic recordkeeping?

Dr. DETMER. Yes. First, I would echo your initial comment, but very strong differences of opinion exist about this issue. Those of us who have actually worked in both the paper era as well as, or have a professional interest in the electronic approach, feel that actually there are a number of advantages to computer-based records. You can encrypt it, you can extract solely the information you are interested in and move it along, otherwise keeping the rest of the record behind. You also have audit trails that can be helpful.

The point is that with the complexity of health care moving the way it is in terms of the technology, the care itself, the medical information and such, I think the only way we will have high quality, cost-effective care is with computer-based record systems. And, as a country, we have not done what we could do to move this technology forward.

A key requirement for progress in this technology relates to what we are here today for—privacy legislation is an absolutely essential foundation brick needed if we are to see the real benefits of this technology develop.

[The following was subsequently received:]

In its administrative simplification requirements, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)(Public Law 104–191, Aug. 21, 1996) calls for uniform standards for electronic transactions in health administration precisely because separate standards developed at other than the national level are not workable.

The Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996 (September 11, 1997), noted that

[t]here is continuing movement toward a computer-based patient medical record, with national standards for content and format, and the possibility of ready interstate transmission as needed for patient care. A major impetus toward adopting this type of record was a report of the Institute of Medicine in 1991 that recommended adoption of the computer-based patient record as the standard for all patient care records. Likewise, increasing use of telemedicine means that patient information will often cross State lines, sometimes in real-time delivery of care. This promising development is an important facet of the National Information Infrastructure because of its potential to provide greater access to quality health care for all Americans, especially those living in rural and remote areas.

The National Committee on Vital and Health Statistics (NCVHS) last year held six days of hearings involving witnesses from the full spectrum of public and private constituencies concerned with privacy, consumer interests, and operation of the health care system. Testimony received at these hearings showed that ''computers are perceived both as threats to patient privacy and as tools for protecting personal health data. Some see computerized information as the best way to support greater use of data without revealing patient identifiers. With traditional paper records, for example, the difficulties of creating non-identifiable data are typically significant. It may be impractical and very time-consuming to make a complete copy of a paper record with all identifying data removed. With a computer record, the administrative burden of creating anonymized records may be insignificant. Others see computerized repositories of health data as magnets for hackers and other abusers.'' Further testimony suggested that

[T]he real threats to computerized information—as with paper records—come from insiders and not from hackers.

Nevertheless, because of the important and increasing role of computers in health care, it is important to be sensitive to both public perceptions and to the possibility that abuses of computerized health records will increase in the future. One response would be increased criminal and civil penalties for misuse of computerized health records. These penalties should apply to both inside and outside abusers of health data.

The Committee noted that it is often overlooked that computers contribute directly to improved patient care in many ways, and that debates on the proper role of computers and electronic records often focus only on the threats to privacy and not the benefits for patients. The committee concluded that a more balanced discussion about the value and the risks of computers is essential, and

that we need to do more to develop and implement technological protections for health records. Technology offers the possibility that we can use records for socially beneficial purposes while fully protecting privacy at the same time. Greater use of nonidentifiable, coded, or encrypted records can make everyone better off at little or no cost. Technology will not cure all problems related to the use of identifiable information, but it can diminish the intensity and scope of the problems. This may be the most promising area for additional development.

The NCVHS has not addressed incentives or disincentives for the keeping of electronic records. A new NCVHS workgroup on Computer-based Patient Records may address this issue in the future.

Chairman THOMAS. Let me ask the question a slightly different way. Are our efforts enhanced, do we make the job easier or more difficult based upon the way we approach how we are going to legislate; that is, try to deal with the very sensitive question of privacy for both individually identifiable records and encrypted records, whether they be electronic or paper; or if we put a serious emphasis on trying to create a timeline in which we move to the electronic era and then deal with the same concerns about individ-

ually identified records? I am wondering which, in your opinion, would get us there in the most efficacious way.

Dr. DETMER. I think if we acted on this issue—if you acted on this issue in this session——

Chairman THOMAS. I assure you it is going to be "we."

Dr. DETMER. Well, I would hope so. In any event, if this is acted upon in this session, I honestly think the field is moving forward, but there are also things that would be in the public's interest that the Congress could also do to facilitate the development of computer-based health records.

We have in this country fairly well-developed hospital information systems compared to those for primary care and smaller care units. If you look at the United Kingdom or the Netherlands, for example, they have put in some tax benefits as well as equipment writeoffs that really have moved that technology forward.

And, incidentally, they have privacy legislation in place, and the populations in both of those countries feel quite good actually in that sense about this issue. I am not saying to every last person, but as a development I think it is seen as a positive thing.

Chairman THOMAS. The difficulty, of course, is that Great Britain is a unitary country and we are a Federal system, and States have proper roles to play in a number of areas. Dealing directly with individuals, for example, with regard to health and welfare, is one of the roles the States have to play which makes our job more difficult to bridge those differences.

In looking at the information, one of the concerns I think is warranted by the individuals who do not want to err, who are concerned on the side of the right to privacy, is the access to those identifiable patient records. Does it seem reasonable that if we, for example, move toward a system which would allow for a determination of who accessed the records, to make that accessing of the records available to individuals?

I know you can place extreme punishment on people misusing that information. But I think the most chilling effect often on people misusing that information is to make it easily known as to who it is that is accessing those records. That is the first part of the question.

The second part, since that involves enforcement in a very direct way, it is too simplistic to view the role of the Federal Government and the State legislators as perhaps dividing it along that line; that where there are identifiable personal records, that could be a very proper and appropriate role for the States to deal with how you deal with that information; and the encrypted records, primarily for research, far more often travel across State lines, are collected for purposes that should have a set of protocols properly approved by an appropriate agency? Is that too simplistic a view?

Dr. DETMER. The difficulty, unfortunately, is we have been getting testimony in some of our recent hearings in particular that the ability to assure the data are securely encrypted, clearly identifiable, or are clearly not identifiable is not likely to be that airtight.

The fact of the matter is, almost all of these things can be open to manipulation, if you will. The most likely assurance you will be getting encrypted or nonidentifiable data, which involves a lot of the information, will simply be from the fact that you have strong

sanctions in place. People will clearly want to just use nonidentifiable data as much as possible to avoid, obviously, the exposure to sanctions for misuse.

It would be tough to get back directly to your question, to craft language in that kind of a dichotomous approach.

Chairman THOMAS. But would you respond directly to the point of having the ability to have a clear trail from the identifiable electronic data and providing it to, for example, the individual, as to who it is that has been looking at the records?

Dr. DETMER. Yes, I think certainly the trail, the idea of audit trails is a protection. It is also true, of course, depending on how much information you keep relating to all the trails and who is involved, that that also then becomes, if it is overdone, yet another set of information that could then be abused and hence invade privacy. So all of these things have a balance that has to be struck.

[The following was subsequently received:]

The NCVHS provided its recommendations on adoption of security standards in a letter to the Secretary, HHS, dated September 9, 1997. In providing a series of principles and recommendations for the Secretary's consideration, the Committee stated that in order for health information systems to be secure, there must be monitoring of access. Specifically, ''[o]rganizations should develop audit trails and mechanisms to review access to information systems to identify authorized users who misuse their privileges and perform unauthorized actions and detect attempts by intruders to access systems.''

Chairman THOMAS. And then finally, I know it was in your testimony but I want to underscore it, the administration in making its initial proposals placed a privileged category for law enforcement agencies, and you voiced some concern about that.

My assumption is we all understand the importance of that, but that in your opinion they probably carved out too big an island, too exclusive an approach for law enforcement?

Dr. DETMER. Yes. With all respect, this was the only area of significant difference between the committee's recommendations and the Secretary's recommendations. We urged substantive procedural protections. We felt law enforcement should justify their need for personal identifiers, remove those identifiers at the earliest possible moment, unless needed for fraud investigation, and a court order seemed appropriate for access.

There was a huge array of issues we had to look at. We did not spend a detailed amount of time on this, and probably will deserve to spend more, but clearly we did differ from the Secretary in that and we urged more protections.

Chairman THOMAS. Thank you very much, Doctor. Obviously, we will rely on you in your ongoing examination. My belief is this is an area that could change relatively quickly in terms of techniques that are being developed, especially when we are looking at an August 1999 deadline. At least, I certainly hope so.

Thank you very much for your input.

Does the gentleman from Wisconsin wish to inquire?

Mr. KLECZKA. With respect to research currently being done by managed care companies, is that being done with the informed consent of the individuals?

Dr. DETMER. Right now we have very much a patchwork of incomplete and inadequate protections generally. I think most managed care companies do in fact—and health care organizations—do in fact try to protect the data of patients. Obviously, we do not have full information. In fact, one of the problems of this whole field is a relative lack of the kind of research base that would be very useful to us as a committee, as well as to you in your roles.

In general, if you have health professionals involved in the work, whether it is the quality work or cost effectiveness or whatever, utilization work, health professionals have a genuine concern for confidentiality. And I am not sure it is always done ideally by health professionals, but it has been part of their upbringing from the time they got into the health professions. There is a bit perhaps less dedication and concern for privacy as you get beyond the health professionals themselves.

[The following was subsequently received:]

We do not know. The Committee does not have information on this area.

Mr. KLECZKA. Later this year the European Union is scheduled to come down with a directive relative to transferring of data to a third country, and that directive indicates that they want to ensure the level of protection. Currently, does this country meet the criteria that is set forth in that directive?

Dr. DETMER. It is not precisely clear to me that it does. If you really look at it pretty literally, I would say it does not. This is not a formal committee view, that is my own assessment of this. The committee has not formally assessed the matter.

But I do think it is important for us, and it does speak to the issue of States' preemption. If we do not have a Federal law that is sufficiently recognizable as a national standard, we certainly could be open to the clear interpretation that we would not be meeting the EU guidelines, and it would prevent us from being able to share information for purposes of research and other social benefit.

[The following was subsequently received:]

The EU directive is a very comprehensive privacy law covering all personal data and designates an official with power to regulate private sector use of personal data. The U.S. does not have a comprehensive legal scheme of data protection, nor an official who has privacy protection as a sole responsibility on a nationwide, or government-wide basis. Rather, it has a number of separate State and Federal laws, but no privacy law generally applicable to all data.

Mr. KLECZKA. What would be the impact on this country in terms of trade and research should we not meet the criteria and so forth in the directive?

Dr. DETMER. I have not seen specific estimates, but in terms of looking certainly at drug development and other activities that are in the public's interest, I think it would have an adverse impact on what would otherwise be a desirable thing.

[The following was subsequently received:]

The impact is not yet clear. It is our understanding that the Commerce Department and the State Department have been involved in discussions with EU staff. Within the Department of Health and Human Services, the HHS Data Council is surveying its staff and operational divisions to determine the extent to which individually identifiable personal data moves from the EU to the U.S.

Mr. KLECZKA. It is your view, at this point at least, we do not currently meet the specifics of that directive?

Dr. DETMER. That is my own personal interpretation, yes.

[The following was subsequently received:]

We believe that the U.S. may not currently meet all of the criteria of the EU directive.

Mr. KLECZKA. What is the timing of that? It is supposed to come down later this year?

Dr. DETMER. I do not know the specific time. I could get back to you on that, but it is coming along, though, that is for sure. But exactly specifically——

Mr. KLECZKA. I have information the effective date is October of this year.

Dr. DETMER. You sound like you have the information.

Mr. KLECZKA. Thank you very much.

Chairman THOMAS. Does the gentleman from Louisiana wish to inquire?

Mr. MCCRERY. Just a couple of questions, Mr. Chairman.

Dr. Detmer, I want you to expound a little bit on the question of preemption of State laws. I am a little concerned about what I perceive to be the Secretary's recommendation that we have a national law, a national standard, but that we allow the States to enact stricter standards.

How is that going to solve the problem of uniformity? It seems to me to be contradictory. Can you expound upon that?

Dr. DETMER. Well, this is a very complex issue. The committee, to the extent it has spoken to this, feels like it is worth splitting out this issue and not looking at it in a totally either all Federal, no State, or wide open and a weak Federal floor, if you will.

There may be areas where it might be very wise to in fact allow State standards. For example, the area of public health law. The States have very well-developed public health laws that have been developed in very good collaboration with the Federal Government. So I think our general attitude would be you should look at preemption piece by piece.

Speaking personally, you are going to be hearing from a witness from Minnesota. If you do see, as the Chairman said, States doing too much experimentation, 50 points of light in my view is not necessarily going to give us enough clarity on this. If you have a sufficiently high standard, the States will not seek to do more. In some areas, like public health law, it is probably the best approach to acknowledge that body of law.

[The following was subsequently received:]

Preemption of state laws was the most difficult conflict identified at the hearings we held, and did not yield a clear answer. The NCVHS addressed preemption specifically in its recommendations to the Secretary (June 27, 1997), as follows:

Among large segments of the health industry, a major benefit to federal legislation is a high degree of regulatory uniformity throughout the country. The interstate nature of health care treatment and payment activities is readily apparent. It will be difficult for many involved in electronic transfers of health data to accept any proposal that does not offer significant relief from the prospect of 50 different state laws establishing separate rules.

On the other hand, it would be difficult for many patient groups, privacy advocates and perhaps some provider groups to accept any proposal that does not allow states to adopt stronger privacy protections as specified in the HIPAA. People disagree whether existing state laws offer greater protection than most of the current federal proposals, but a proposal is not a law so judgments in this area are premature. There is strong support in some communities for a minimum federal confidentiality standard that allows states to erect stronger privacy barriers. HIPAA already reflects a policy that stronger state laws should be allowed to prevail.

Existing proposals differ on preemption. Most preserve existing state mental health and public health laws, but the scope of this language is unclear. H.R. 52 adds a new idea to the mix by allowing states to pass additional restrictions on access to health records by state officials.

The Committee suggests, however, that this issue need not be treated as a single problem with a single solution. The conflicts need to be broken down into components, and each component analyzed separately. In some areas, the case for federal preemption may be stronger. For example, it may be unnecessarily complex to support 50 different patient access procedures. On the other hand, the need to recognize the diversity of state public health laws is already clearly reflected in most proposals. No one has suggested or is likely to support a uniform federal public health law. A narrower and careful analysis of preemption may help to minimize the admittedly strong conflicts here and may point to more effective resolutions. However, if sufficient national conformity is not achieved, both national and international objectives cannot be met.

Mr. MCCRERY. Can you briefly, if you feel comfortable doing this, either on the part of the commission or on your own part, outline for us the reasons for having a national standard?

Dr. DETMER. Well, I think clearly the most critical one in my view, speaking as a practicing physician and looking at the fact that much of the population in this country lives near State borders, if we have stiff penalties in place, let us say a patient works in the District, lives in Virginia, and gets their care in Maryland. You will have different States which will have different standards, with still very stiff Federal penalties. Trying to keep that straight, both as a patient and as the provider, it strikes me as really making it very difficult, and we do want to have an effective law.

If I were just to speak to one thing, that is, in my mind, one of the most compelling arguments to be made for strict Federal preemption. But, again, I would be happy to try to get back to you with more specific direction on this very important issue. Without question, it is one of the more controversial areas of this legislation.

[The following was subsequently received:]

The existing legal structure does not effectively control information about individuals' health. Federal legislation, establishing a basic national standard of confidentiality, is necessary to provide rights for patients and define responsibilities for record keepers. The Committee's position on this is reflected in its recommendations to the Secretary (June 27, 1997) wherein it made a number of principal findings:

The United States is in the midst of a health privacy crisis. The protection of health records has eroded significantly in the last two decades. Major contributing factors are ongoing institutional changes in the structure of the health care system

and the lack of modern privacy legislation. Without a federal health privacy law, patient protections will continue to deteriorate in the future.

The importance of trust in the provider-patient relationship must be preserved. Patients must feel comfortable in communicating sensitive personal information.

Delays in passing privacy legislation will allow additional and uncontrolled uses of health information to develop. Failure to address health privacy will also undermine public confidence in the health care system, expose patients to continuing invasions of privacy, subject record keepers to potentially significant legal liability, and interfere with the ability of health care providers and others to operate the health care delivery and payment system in an effective and efficient manner. The greater the delay in imposing meaningful controls on inappropriate use and disclosure of identifiable individual information, the more difficult it will be to overcome institutional resistance to restrictions on use and disclosure or changing the way that information is acquired and used. On the other hand, the confidentiality of the provider-patient relationship and the confidentiality of health records had been the foundation by which the health care system helps ensure the best possible health care. It is not easy to strike a fair balance between these some times competing concerns.

Mr. MCCRERY. Thank you. That would be helpful, because looking over your testimony, it is not real clear to me, anyway, what your recommendation is.

Dr. DETMER. OK.

Mr. MCCRERY. If you could be more specific, that would be very helpful.

Second question. You talk about needing to guard against discrimination in a number of areas, including insurance. Most people, when they apply for insurance, are they not asked to reveal any health conditions that would have an impact? So what is the problem on discrimination in insurance?

If you see that as a problem, perhaps we should move to some sort of community rating. That would resolve that. Do you want to comment on that?

Dr. DETMER. We have not talked about the issue of community rating as an issue per se. I do think that the very concept of health insurance, though, is it is to be something that is there for people when they are sick. And if indeed you reveal you have illnesses and then you cannot get any coverage, or it is so extravagant or expensive you cannot afford it, then the very concept of insurance is not there.

At some level this is a very important question and is obviously a question that goes beyond the privacy legislation, certainly, but I think it is a very critical question: Do people get coverage for effective services or not? That is a community rating kind of issue.

[The following was subsequently received:]

To the extent that the NCVHS has addressed this matter, its discussions have included the following points. The relationship between privacy (as defined by principles of fair information practices) and discrimination is an issue that was raised a number of times during the NCVHS hearings last year. Some motivation for protecting health information is to prevent the discriminatory use of the information both inside and outside the health care setting. Patients receiving care for some health conditions or who have been the subject of genetic testing have been and continue to be the subject of discrimination in employment, insurance, and elsewhere. Several current Congressional bills address the possible discriminatory use of genetic information.

Discrimination based on health status and condition remains a major and important concern. While the Committee has not focused its full attention on discrimination, legislative responses are appropriate. It is not clear, however, that general pri-

vacy concerns and discrimination concerns must be or should be addressed together in the same piece of legislation. An already complex health privacy bill is not the best place to sort out responses to equally complex discrimination problems. The Committee suggested in its recommendations to the Secretary (June 27, 1997) that privacy and discrimination issues deserve separate legislative treatment. The problems of discrimination are important, but not enough work has been done to explore the content of anti-discrimination legislation. The Committee urged the Secretary to propose legislation expanding the anti-discrimination provisions of HIPAA to cover all aspects of discrimination based on health status and condition.

Mr. MCCRERY. Thank you.

Chairman THOMAS. Does the gentleman from California wish to inquire?

Mr. BECERRA. Let me ask a question, and this may be somewhat premature, since we are trying to figure out what we believe confidentiality or privacy to be and how we address it, but certainly some of what we want to protect will have to be done through statute.

The preemption issue, for example, makes it clearly Federal versus State. We will have that dispute. But some areas are probably best protected by regulation because they may need to change periodically and statutes would be too difficult to have constantly amended. Do you have any sense right now, Dr. Detmer, what areas are clearly best left to regulation versus statute? What should we not do?

Dr. DETMER. That is a very tough question and it is one, obviously, I think all the Members of the Subcommittee grappled with. I do not question at all the validity of your basic comment. It is true that if you put too much in a statute, you do not have the flexibility that can come with regulation.

Clearly, I think we do need a set of basic health information practice protections, and those, I think, can be a matter of statute. Exactly how those play out over time are appropriately left to regulation. And certainly as the chair of the national committee that has with a nearly 50-year history of advising government, I think that the NCVHS committee review process is a wonderful mechanism by which regulation can became more attuned to the times and the needs.

Here is a group of private citizens serving and giving expertise to the Government, having an opportunity to hold hearings for wide varieties of folks and then making recommendations. The HIPAA legislation in that regard is a very nice model, because it did lay out a general picture, but then it also mandated that regulations would follow based on explicit hearings and the advice of this Subcommittee.

Mr. BECERRA. Is there any particular area you could identify for us?

Dr. DETMER. Well, I say certainly basic health information practices. I will be happy to get back to you. I think it is a very relevant and critical question actually to the legislation.

Mr. BECERRA. I think to the degree you can help us set the parameters of what we are going to do, if there is something we should clearly leave off the table with regard to statutes and limitations, it would help us quite a bit.

Dr. DETMER. Certainly.

[The following was subsequently received:]

Both the NCVHS in its recommendations to the Secretary (June 27, 1997), and the Secretary in her recommendations to Congress (September 11, 1997), recognized the difficulty in drafting health privacy legislation and recommended a "safety valve provision." Specifically, the Secretary's recommendations noted:

We recommend that there be authority to suspend, by regulation, any provision of the legislation for a limited period in the event of an unforeseen significant threat to health or safety, significant threat to patient privacy, major economic disruption, or manifest unfairness.

The design of precise controls on the use and disclosure of information is a complex task, and it is possible that the legislation would forbid a disclosure, or otherwise constrain behavior, in a way that causes unanticipated hardship.

Authority to suspend a provision would ensure that situations like this could be addressed, on a temporary basis, pending Congressional consideration of amendments.

Federal agencies are accustomed to the flexibility provided by the Privacy Act of 1974, whose routine use provision (5 U.S.C. 552a(a)(7) and (b)(3)) permits agencies to make administrative choices to disclose information beyond the disclosures explicitly allowed in the statute. We do not recommend administrative authority as flexible as the routine use provision, which appears in a law covering all activities of all Federal agencies, and where a statutory catalog of all possible uses of information was not feasible. We recommend a provision to deal with extraordinary situations that may have not been foreseen, and then only for a limited time.

Mr. BECERRA. With regard to the whole issue of the data we collect and how we keep all that information, electronic, paper, and so forth, what do you do with the nonprofit, the community-based clinic that already survives on a shoestring budget, if we determine that the best way to keep information safe is to go toward some electronic mechanism?

How do we help those that are barely surviving to provide health care, to now get to the point where they will abide by statute or regulation requiring them to provide protection to private information?

Dr. DETMER. Very good point. It came up in our hearings. In particular, we had a hearing out in San Francisco where Los Angeles County Hospital came and said, Look, our budgets are so low, the idea we can have a very wonderful, which we would like, information system with what many of you might consider really important and basic information is simply beyond our means.

There is clearly cost involved in this issue, and certainly one of the main drivers of HIPAA was to in fact save money from administration simplification. We again lack the facts and data that would allow us, I think, to really know exactly how big a problem this will be. We know in some areas trying to do much of anything would probably stretch their budget. So there is a tension in here and there is a cost in this.

On the other hand, there is also a general public concern about privacy. We need to have a law but we do need to, I think, look carefully at the costs that that will impose on people.

[The following was subsequently received:]

Section 1173 of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191, Aug. 21, 1996) requires the Secretary to adopt standards for electronic data transactions, but does not mandate that providers exchange information electronically. While issues regarding costs of maintaining and providing information electronically have been raised at its hearings, the Committee has not addressed this issue.

Mr. BECERRA. Thank you, Mr. Chairman.

Chairman THOMAS. In regard to that, though, the next panel will have some comments, and I find the argument on cost a bit analogous to the preventive care arguments we had, that wound up with us finally spending money according to the budget rules. Everyone involved believed that in the long run, a decade, a generation, that we would save money on preventive care. With adequate records, the investment and the ability to keep really accurate records, that a number of areas such as duplicate procedures or missed procedures, that would save customers in the long run, may very well be at least offsetting.

That is not a comfort to someone who has to meet a budget on a quarterly or a yearly basis, but we need to look at all aspects of the decision rather than just very narrowly someone's quarterly accounting on the cost of changing the way in which we provide records both to the patient and to the system.

The other point I wanted to make before I ask you a final question, the gentleman from Louisiana's line of questioning is very, very pertinent, and I have had an ongoing, mostly positive relationship with the insurance business trying to convince them that their real job is to manage risk, not eliminate risk.

Dr. DETMER. Thank you.

Chairman THOMAS. Under the current rules, at the same time, we ought not to shoot the messenger if what they do is provide us, under the current rules, the cost of coverage for particular concerns. That then becomes an immediate problem for the individual, but it becomes a problem for society in examining the way in which the current rules operate.

And that goes to the gentleman from Louisiana's discussion about community rating or getting better risk assessment tools available to us for making these kinds of decisions, because I do not want the industry to pull punches in terms of what the costs of these various conditions would be to insure in the current world. That allows us to make a realistic decision and not an unrealistic one.

Then, finally, as we get into this area which all of us now I think are fairly sensitized to, as to its importance in dealing with privacy, we do not have a comprehensive privacy statute on the books. The string theory of physics for privacy, I think for a very good reason. We do have, though, a number of statutes on the books, and the staff has listed for me the Privacy Act of 1974, Americans With Disabilities Act, the Controlled Substances Act, and most recently, the Balanced Budget Act.

Did the committee review those? And can you give us any lessons learned from the implementation of these earlier Federal statutes, in terms of their either applicability or the difficulty of converting?

One of the things we do around here is take something that has worked in the past and apply it to something else. Do you have any cautionary words about the way in which we might approach this particular area of privacy vis-a-vis what we have done in the past and what might be seen as somewhat similar or related areas?

Dr. DETMER. Yes, and the committee has not explicitly dealt with that question, particularly the Balanced Budget Act, which is very current. I think the question is a good one and one that I will put to the committee. I think it could be useful to you to get back on that.

In general, as an offhand comment, I do not think that the process, being the way it operates, it has been that bad. In fact, it has been quite good.

I do want to respond to an earlier comment, if I might. I think my first time to ever testify before you was soon after I had chaired the Institute of Medicine study on computer-based patient records some years ago, and I want to underscore how much I agree personally with what you are saying here. On the basis of that study and other work, we will not get to truly value-based, cost-effective care, even looking at these issues of cost on insurability and such, until we have much finer grain reliable information. That is only going to come actually out of computer-based analysis, properly done, with the appropriate confidentiality protections in place.

[The following was subsequently received:]

The Committee has not examined the Privacy Act or the other laws in any depth in developing its recommendations.

Chairman THOMAS. Well, without it I do not see how we can create some outcomes research that providers will need, that we will need as smart buyers with the taxpayers' money, but, more importantly, providing a body of information to patients so that they can be smart consumers as well, which is one of the fundamental ways we will keep a control on health care costs.

Dr. DETMER. Many of us are grateful for your leadership on that.

Chairman THOMAS. The final comment would be to tie in once again with the gentleman from California. While you look at these various particulars, the other thing I am most concerned about is the balance between statute and regulations. Because, obviously, given the changing technology, we are not going to be able to write a piece of legislation that is probably as flexible as we would like for the near term.

If you could, create some bright lines for us that would be most appropriate in legislation versus areas that probably are going to be changing and we can review, lock up if necessary in legislation in the future, but perhaps might lead to legislation.

My real worry about that is that as this argument for privacy continues, I do want to make sure the Federal statute encompasses the basic structure so that there will not be, for want of a better term, an end run around what we are trying to do by—particularly by States being overly zealous in regulating beyond what is necessary to create those clear and necessary personal privacy and confidentiality protections, but still allowing for the collection of

data which will allow us to move forward, both for individuals and for medical science.

[The following was subsequently received from Mr. Detmer:]

As noted above in response to Q9., both the NCVHS recommendations to the Secretary (June 27, 1997) and the Secretary's recommendations to Congress (September 11, 1997) recognized the difficulty in drafting health privacy legislation and recommended a "safety valve provision." The Secretary's recommendations specified that "[w]e recommend that there be authority to suspend, by regulation, any provision of the legislation for a limited period in the event of an unforeseen significant threat to health or safety, significant threat to patient privacy, major economic disruption, or manifest unfairness."

Any Members have any additional questions?

The gentleman from California.

Mr. BECERRA. Really quickly, and again this may be premature, was there a great deal of discussion of what you do after privacy information has been disclosed? What about the person who has a mental history and those records are disclosed, or has the AIDS, HIV virus? What happens in that case, when the cat is out of the bag? Did you propose or discuss what should be the remedy in those cases?

Dr. DETMER. Well, I think we do see, as I say, sanctions that should come into play if there are obvious cases of that type. You mentioned both mental health as well as HIV, for example. Clearly, there are some sets of health information that will expose people more than other general data, like a simple blood pressure, pulse reading, say.

The general feeling is that if you really start taking it case by case and trying to look at genetic information, or HIV status, or mental health data, all in separate kinds of all special sorts of cases, that becomes something almost impossible to try to manage sensitively and appropriately. The committee's general feeling is, Let us put in a very good standard and let us have that standard be such that it protects those people, so that in fact your protection does not depend on what disease you unfortunately happen to get or what problem you happen to have.

Mr. BECERRA. If I could ask this, as you all continue, if you could give some close attention to giving us some strong and specific recommendations on sanctions, because there will be all sorts of special interests in this trying to fight to either make them very strong or very weak, and it would help if we had some good guidance from those who are examining the whole issue. Give us a sense of how strong or how weak we should be with regard to sanctions, if in fact we find that information is disclosed.

Dr. DETMER. It is clearly a judgment call. At least I would advocate that you make them sanctions that really look and feel like sanctions, if it looks like a horse and feels like a horse. I really think that needs to happen.

I think they really need to be there, but it is still a question of levels. And you are right, there will clearly be some pressures to make it higher or lower. Again, I will see if I can try to give you some advice on that, if I can.

[The following was subsequently received:]

There is clear consensus that there be strong civil and criminal sanctions. A federal privacy law should, as recommended by the Committee (June 27, 1997) and the Secretary (September 11, 1997), "provide for punishment for those who misuse personal health information and redress for people who are harmed by its misuse. There should be criminal penalties for obtaining health information under false pretenses, and for knowingly disclosing or using medical information in violation of the Federal privacy law. Individuals whose rights under the law have been violated should be permitted to bring an action for damages and equitable relief."

Mr. BECERRA. Thank you, very much.

Thank you, Mr. Chairman.

Chairman THOMAS. Looked like a horse and kicked like a mule.

The key to that is where it is personally identifiable and it is electronic, you will know who has done it with the audit trail, and that you allow for relatively tough sanctions but the court system to resolve a number of those on the intensity.

We obviously have access to taxpayer funds for medical purposes to sanction a number of people who are involved in the medical end of it through research or other ways, and a combination of those are what we are going to have to look at.

Dr. DETMER. It is not as though we have no protections or things in place at this point. In fact, I think there is quite a bit of interest and commitment to this. It is just that we do not have a privacy law.

Chairman THOMAS. And to determine which ones appropriately match up.

Dr. DETMER. Exactly.

Mr. BECERRA. The bottom line is, for the patient who has had this information exposed, there is little remedy he can do in terms of money or some type of civil or criminal sanction against that disclosure to make that person now feel whole.

I would think we would want to construct something that provides swift sanctions and, as you said, it really has teeth. Because what you want to do, as you said before, is protect the information from ever being disclosed, especially information that is that sensitive of a nature.

Chairman THOMAS. The gentleman is pursuing a line of deterrence. I understand what you are saying.

Mr. BECERRA. Prevention.

Chairman THOMAS. You probably would not want to go down that road in other areas of discussion, but I clearly think a good example would be a deterrence. If you have a clear indication of someone violating it, a relatively swift and stiff punishment would occur, and we will explore those avenues.

Dr. DETMER. And, in fact, unfortunately many lapses are essentially a person who has no business doing what they are doing. And that is far more the more common area than a problem with the technology itself or something else. It is somebody not respectful of these kinds of data and the personal harm they do to people.

Chairman THOMAS. Well, thank you very much. This is obviously the beginning of a process of producing legislation that will both protect individuals' right to privacy and confidentiality of records

and also allow us to continue to access them for legitimate medical and research purposes.

Thank you very much, Doctor.

Dr. DETMER. Thank you.

Chairman THOMAS. We can ask our next panel to come forward.

This will be Dr. Stephen Borowitz, who is associate professor of pediatrics and health evaluation sciences at the University of Virginia, Charlottesville; Janlori Goldman, director of the Health Privacy Project at Georgetown University; Dr. James R. Birge, I believe it is, medical director and chief executive officer of the MacGregor Medical Association in Houston, Texas.

Dr. Borowitz, a copy of your full statement will be placed in the record. You may proceed in the time available in any way you see fit.

STATEMENT OF STEPHEN M. BOROWITZ, M.D., ASSOCIATE PROFESSOR, PEDIATRICS AND HEALTH EVALUATION SCIENCES, UNIVERSITY OF VIRGINIA HEALTH SCIENCES CENTER, CHARLOTTESVILLE, VIRGINIA

Dr. BOROWITZ. Mr. Chairman and Subcommittee Members, my name is Stephen Borowitz and I am associate professor of pediatrics at the University of Virginia. In the next several minutes I hope to show you how information technology can improve health care.

The practice of medicine is information intensive. Forty percent of hospital operating costs result from patient and professional communications, and physicians and nurses spend as much as half of their time documenting. Yet 70 percent of the time, physicians do not have all the information they need. The greatest reason for this is that we continue to keep most medical information in a paper medical record.

The paper record today is little different than 50 years ago, despite an explosion of medical knowledge and technology. Information is not sorted for relevance but rather by source and chronology, so that critical information may be deeply buried. Increasingly, the paper record is serving purposes it was not designed for. It is the source of medical billing documentation and the principal repository for medical-legal information. There is more and more information in the record, much of which has little or no direct clinical relevance.

When compared to paper records, computerized records provide easier and faster access to clinical information. The data are of higher quality, always legible, and can be displayed in a number of different formats. Many organizations are already developing computer-based records.

This is my younger daughter's record at the University of Virginia. This and other systems are searchable. We can search for all of the patient's blood counts, and the results are displayed quickly on a single screen and can be graphed or analyzed. The system also contains text.

This is a hospital discharge summary of a little girl with ulcerative colitis whom I care for. Two days after her hospital discharge she returned late at night with intestinal bleeding. Because of this computerized record, the emergency room physician immediately

knew her problem, who should be contacted, and what interventions were appropriate.

Computerized records can contain images such as x rays or electrocardiograms. By being able to view this old electrocardiogram, an emergency room physician can determine that this man complaining of chest pain is experiencing heartburn not a new heart attack.

Perhaps the greatest limitation of the paper-based medical record is that it actually does not exist. Every health care provider who has ever seen a patient has a separate paper record, and these records are viewed as personal notes or reminders rather than part of a larger whole. They are often perceived as owned by health care providers rather than by the patient.

An excellent example of the limitations of the paper record is childhood immunizations. These are the safest and most cost-effective health interventions. Ninety-five percent of children begin the recommended series, and 97 percent are fully immunized upon entry into kindergarten. However, only half of 2-year-olds are fully immunized, yet they are the group at greatest risk for the diseases we are trying to prevent. The number of completely immunized 2-year-olds would go from 50 to 85 percent if we eliminated all missed immunization opportunities.

The biggest barrier to this is the lack of data. Many children change providers or are seen by multiple providers. Half of all children receive immunizations at two or more facilities. This makes responsibility for immunizations ambiguous. Who keeps track of them and who should be responsible?

We have attempted to provide this type of information with Project Vaccine, a shared computerized immunization data base. Here is my younger's daughter immunization record. She is up to date. While this system can recommend immunizations, providers were resistant to this, so we provide current immunization schedules. Over the past 3 years, the rate of completely immunized 2-year-olds in central Virginia has risen from 58 to 78 percent.

In addition to recordkeeping, information technology is influencing the way health care is delivered. For the past 2 years, we have been providing electronic mail consultations across the World Wide Web. Here is the e-mail form directed to me. There is a disclaimer that the information is being conveyed across the Internet and may not be secure or confidential.

Over the past 24 months, I have received more than 1,000 consultations. Here is an example from a parent in rural North Carolina whose 1-year-old son had chronic abdominal difficulties. Nearly 80 percent of my consultations have been initiated by parents. I have received requests from 38 of the 50 States. Clearly, many people out there are seeking information.

I believe information technology is helping to disseminate and redistribute medical information. Information that was previously only available to medical professionals is now available to anybody with access to a computer. This can only help patients and their families to be more active participants in their own health care and to make better and more informed health care decisions.

Thank you.

[The prepared statement follows:]

Statement of Stephen M. Borowitz, M.D., Associate Professor, Pediatrics and Health Evaluation Sciences, University of Virginia Health Sciences Center, Charlottesville, Virginia

Mr. Chairman, Members of the Subcommittee on Health, thank you for your examination of two crucial and intertwined issues confronting our health system: the confidentiality of medical information, and the use of computer and communications technology to improve patient care. My name is Stephen Borowitz. I am a pediatrician who specializes in gastroenterology and nutrition and an Associate Professor of Pediatrics and Health Evaluation Sciences at the University of Virginia. I have long had interests in how information technology can be used to improve the delivery of health care as well as the delivery of medical education. My task today is to give you some idea as to the potential of information technology to improve the coordination of and access to health care, and help physicians and other health care providers become lifelong learners.

While I speak today as an individual physician, I must note that the explosion of information technologies is reaching deeply into every corner of our nation. Today health data can be transferred from facility to facility in seconds, read and interpreted hundreds or thousands of miles away from the patient, stored on a variety of disks, drives, tapes, etc. In health care the global village is rapidly arriving, and patients in that global village could live in the smallest town in rural Virginia or across the world, and be treated by specialists at our Health Sciences Center through the use of telemedicine and other technologies.

I am also a member of the American Medical Informatics Association (AMIA), a national organization dedicated to the development and application of medical informatics in support of patient care, teaching, research, and health care administration. AMIA's more than 3800 physicians, researchers, librarians, information systems managers, and other professionals with expertise in information technologies recognize that the enormous potential for computer and communications technology to improve health care cannot be realized unless individuals and the society-at-large are reasonably certain that safeguards are in place to protect the confidentiality of personal health data in medical records. My comments today reflect not only my own views as a physician who actively uses technology to improve patient care, but also those of many members of AMIA.

The practice of medicine is information intensive. Nearly 40% of hospital operating costs result from patient and professional communication activities. Despite the fact that physicians spend more than a third of their time "documenting," and nurses spend nearly half of their time "documenting," physicians report that 70% of the time they do not have all the information they need to best care for a patient.

Perhaps the single greatest reason health care providers do not have all the information they need to deliver the best care is that we continue to keep most medical information in paper medical charts. Paper medical records have changed little over the past fifty years despite an explosion of medical knowledge and medical technology. While there are clearly advantages to the paper medical record in that it is familiar and portable, this form of record keeping has many limitations. Information in the paper medical record is not sorted for medical relevance. Rather, information in the paper record is sorted first by data source (i.e. medical orders, inpatient notes, laboratory results, radiology results, nursing notes, etc.), and then by chronology. This often means that the most important data elements are buried within the record rather than being one of the first things a health care provider sees when he or she opens that record.

Increasingly, the medical record is serving purposes it wasn't originally designed for. The medical record now serves as the principal source for medical billing documentation and the major repository of medical-legal information. This means that there has been a tremendous increase in the amount of information within the record, much of it with little or no direct clinical relevance.

While there are many potential obstacles to the development of computer-based patient records, such systems can overcome many of the limitations associated with paper-based medical records and offer health care providers better information upon which to base clinical decisions. When compared to a paper-based record, a computer-based patient record provides easier and faster access to clinical information, the data are of higher quality, clearly legible, and can be displayed in a number of different formats. Computer-based patient records can generate prompts and reminders during the delivery of care and provide health care givers with decision support and links the medical literature thus integrating the delivery of care with the educational process.

Computer-based patient records can decrease some of the costs associated with health care. With a completely searchable record, there will be a decrease in the

number of redundant or unnecessary diagnostic or therapeutic procedures that are now performed because of incomplete or incorrect information. A computer-based patient record can dramatically reduce the costs associated with the filing, transporting, and copying the paper medical record and the generation and submission of bills. In large medical centers it costs $8.00 each time a paper record is pulled for use and $11.00 to complete each paper-based billing encounter form.

Perhaps the greatest limitation of the paper-based medical record is that it actually does not exist. The paper-based medical record is based on the construct that people are cared for by a single physician or organization across the continuum of care, throughout a lifetime. Given the complexity of our current health care system and the mobile nature of our populace, no individual has a single "medical record." Rather, every health care provider who has ever seen that individual has a separate paper record, even if many of those health care providers work in the same facility. The information within these disparate and uncoordinated paper medical records is often thought of as personal notes or reminders for that health care provider or health care organization rather than as part of a larger whole. These separate paper medical records are viewed as being owned by the health care provider rather than by the "patient" to whom they pertain.

One of the most illustrative examples of the limitations of our current paper-record based system is childhood immunizations. Childhood immunizations are perhaps the safest and most cost-effective health interventions we currently have. For every dollar we spend successfully immunizing a child, we save $10.00 to $14.00 in the future. We know that 95% of children in this country begin the recommended series of immunizations; the first immunization is now administered before the infant leaves the hospital. We also know that 97% of children in this country are fully vaccinated at the time of kindergarten entry largely because it is required. However, only 37–56% of two-year old children are fully immunized despite the fact that these are the children at greatest risk for the diseases we are trying to prevent. Numerous studies have demonstrated that underimmunization rates among two-year-olds do not vary substantially by ethnicity, geography, socioeconomic status, or health insurance status. Children who receive their health care from private pediatricians are just as likely to be underimmunized as are children who receive their health care from public health departments. Children who have private health insurance through their parents' employer are just as likely to be underimmunized as are children who have no private health insurance. This is primarily due to a lack of reliable information. Many young children are seen by multiple health care providers or change primary care providers during childhood. It has been estimated that approximately half of all children in this country receive their immunizations at two or more unaffiliated health care facilities. This makes the responsibility for administering immunizations ambiguous. Who keeps track of childhood immunizations and who should be responsible?

We know that without any changes in patient behavior, the rate of completely immunized two year old children could be increased from 50% to 85% if the health care system eliminated all missed opportunities for immunization. In order to take advantage of these missed opportunities, health care providers need to have reliable information upon which to base their immunization decisions. A shared immunization repository could provide this information. If information regarding a child's immunization history were readily available to any physician treating that child, immunizations could be administered a timely fashion. We have attempted to provide this information for health care providers in Central Virginia with VaCCINe (Virginia Computerized Childhood Immunization Network) . Preliminary review of the available data from 16 out of 32 child care centers and preschools throughout the Thomas Jefferson Health District of Central Virginia demonstrates that over the past three years, the apparent rate of completely immunized two year old children has risen from 58% to 78%.

There are no longer any technological barriers to the development of computer-based patient records and many institutions have implemented portions of computer-based patient records with varying levels of success. However, there are many political and organizational issues that must be addressed. We must develop reliable means of identifying individual patients while insuring the data in their records are secure and confidential.

There is little evidence that health care providers or health researchers misuse health information. While there are genuine concerns about unauthorized public release of personal information or the misuse of personal medical data by employers, insurers or others to discriminate against or otherwise harm an individual, at the same time it is crucial to recognize that access to all relevant patient-specific health care data is essential for those engaged in the provision of care, or in research to advance medical science and improve human life, or in the direction of public health

programs and the protection of public safety. In the end, legislation governing health information must protect not only the confidentiality of individual medical records but also the ability of health professionals to provide care, conduct research, and prevent disease in a manner that benefits the entire population. Health information standards must thoughtfully and carefully balance the rights of the individual, the capacity of the health care system to provide needed care, and the interests of our nation as a whole.

Issues of security and confidentiality are not unique to computer-based patient records. Paper medical records are far from secure. Paper medical records are often kept in relatively open public areas to afford ready access. Moreover, because of the way information is stored in the paper medical record, it is not possible to "sequester" certain types of information from individuals who have access to that record. Anything that is in the paper record can be seen by anybody. Moreover, there is no means of creating an audit trail of who accesses a paper record, or what they do once they have the record.

A common concern about computer-based patient records is that they may less secure and confidential than paper medical records. However, a computer-based patient record can be made more secure than a paper medical record through the use of authentication and authorization, and the maintenance of audit trails. Authentication refers to a process that verifies the identity of the user. This can be by something the user knows (mother's maiden name, ID, password), something the user has (a key, a smart card, a token), by something related to who the user is (signature, fingerprint, voiceprint), and/or by something indicating where the user is (an IP address, a phone number, a hardware configuration). Authorization refers to a process whereby the information and services a user can have access to are limited based upon attributes of the user, attributes of the data, and/or attributes of the request. Finally, the use of audit trails can serve as strong and important deterrents to breaches in confidentiality if strong enough sanctions are employed. An audit trail is a record of information access events and can include the identity of the requestor, the date and time the request was made, the source and destination of the request, a description of what information was retrieved, and what the reason was for retrieving the information. Organizational policies and practices are at least if not more important than technological mechanisms in protecting health information and patient privacy.

In addition to record keeping and access, information technology is influencing the way that health care is delivered. Quality health care is dependent upon good communications between physicians and patients. Successful communication results in the patient's understanding of the diagnosis and increased compliance with therapeutic recommendations and interventions. In addition to face to face and telephone contact, rapid written communication through electronic mail (e-mail) is now widely available to patients and health care professionals. E-mail can provide patients with a direct means of communicating with physicians and assuring them that their messages are received and read. E-mail provides physicians with the ability to follow-up or clarify advice that was provided during an outpatient visit and messages can direct patients to educational materials or other resources available on the Internet.

As of late 1996, nearly 25% of people beyond 16 years of age in the United States have access to the Internet and at least 15% of the U.S. population was using e-mail. In certain regions, one fourth of patients use e-mail to communicate with their health care providers. Those patients who utilize e-mail to communicate with physicians perceive this means of communication as not only more convenient and faster than telephone communication, but also as increasing their access to medical care.

While e-mail is generally viewed as a good means of communicating simple information and non-urgent requests between physicians and patients (i.e. refilling prescriptions, communicating laboratory results, or making appointments), up to 90% of patients who use e-mail to communicate with their physicians relay important and sensitive medical information electronically.

Beginning in November of 1994, the Children's Medical Center at the University of Virginia instituted a pilot program of providing electronic mail consultations in selected pediatric subspecialties (http://www.med.virginia.edu/docs/cmc/giconslt.html). A disclaimer was included at the top of the form alerting people that since the information contained within the form would be conveyed across the Internet, it might not be secure. All consultation replies included a copy of the original consultation request as well as a disclaimer to the effect that since the patient had not been physically examined and the entire history had not been obtained, the validity of the response might be limited.

Between November 1, 1995 and February 28, 1998, the Division of the Pediatric Gastroenterology at the Children's Medical Center of the University of Virginia received 938 electronic mail consultation requests. During this 28-month period, an

average of 33.5 ± 11 consultation requests was received each month with a range of 14 to 68 requests. There has been a slow but steady increase in the number of consultation requests received each month.

The greatest number of consultation requests were initiated by parents or guardians (79%), however 11% of the requests came from physicians and another 10% came from other health care professionals such as nurses, pharmacists, or respiratory therapists.

85% of the consultation requests originated within the United States. During the 28-month period, consultation requests were received from 38 of the 50 U.S. states. Only 8% of all consultation requests originated in the states of Virginia or West Virginia, which comprise our traditional referral area. 15% of the consultation requests originated from sites outside of the United States; consultation requests were received from 37 different countries. Outside of the United States, the most frequent international source of consultations was Canada, followed by Australia, the United Kingdom, and Argentina.

The large number of consultation requests we received from parents and guardians suggests that their primary health care providers do not always meet a family's information needs, or that they are dissatisfied with some of the information they have received. This dissatisfaction is further highlighted by the observation that nearly half of patients use some form of non-conventional medical therapy, often without consulting with or informing their primary care physician. As a group, parents seeking non-conventional medical therapies for their children are well-educated professionals, precisely the group of people who have ready access to the Internet and e-mail.

Many parents appear to be very comfortable seeking medical information from relatively anonymous "electronic consultants." This form of electronic communication provides people with a means of identifying qualified consultants outside of their local health care system and to communicate with these consultants directly without numerous layers of administrative bureaucracy. According to many of the families who consulted us, e-mail communications with an anonymous "electronic consultant" are less intimidating than face to face conversations with time-pressured physicians. E-mail enabled many parents to ask questions that they were otherwise too timid to ask. This may in part be due to the mode of communication. E-mail is a hybrid between written and spoken language. It allows people to choose their words carefully without the pressures of time or place. Response time with e-mail is substantially shorter than with written letters and yet e-mail offers more permanence than a face-to-face or telephone conversation.

The public's increasing interest in online medical consultation reflects the changing nature of our health care delivery system. The rapid growth of electronic communications has paralleled the shift towards giving patients more responsibility for their own health care decisions. As the public has become better educated, they have become accustomed to seeking information about health care from printed media. It is only natural for them to turn to electronic sources of information such as Web sites and, when they have further questions, to contact web-site authors. More and more people in the United States receive their health care through managed care organizations which limit access to specialists and specialized treatments. This means that patients and their families have new incentives to find alternative sources of expert medical opinion, and when they go outside of their health care network, to seek the most time and cost-effective means of diagnosis and therapy to minimize their own out-of-pocket costs.

Given the complexities of the communication process, there are always potential misunderstandings when physicians and patients exchange medical information. The potential for misunderstandings may be magnified when medical information is exchanged across the Internet. The information could be based upon incomplete or incorrect assumptions, the information could be misinterpreted, it could be incorrect or out-of-date, or it could be more up-to-date than information provided by another physician. Given the wide variation in practice patterns, situations may arise in which an online consultant will disagree with the advice of another physician. In the United States, the law dealing with interactions between physicians and patients over the Internet has not been well defined. Potential legal issues include physicians practicing without licensure in the state or country in which the patient resides, alleged medical negligence, and abandonment of patients should the consultant not continue the relationship.

The availability of vast amounts of medical information on the World Wide Web can have important implications for the future of our health care system. One author has called this "the next transformation in the delivery of health care." This dissemination and redistribution of medical information may influence public perceptions of the standards and quality of care and the nature of the doctor-patient

relationship. Medical information on the World Wide Web can help health care professionals educate their patients, learn more about patients' concerns and fears, and help patients make better and more informed decisions about their own health care.

While information technology is already helping to reshape our health care system, it can also help us change some of the paradigms of health care. In our current environment, the practice of medicine, continuing medical education, and clinical research are separate and somewhat independent enterprises. The innovative development and use of information technology and computer-based patient records can help us integrate clinical care with clinical research and lifelong learning while helping patients and their families to be more active participants in their own health care and make better and more informed decisions.

SELECTED REFERENCES

1. Bertakis, K.D. The communication of information from physician to patient: a method for increasing patient retention and satisfaction. J Fam Practice 1977:5;217–222.
2. Coeira, E. The Internet's challenge to health care provision. BMJ 1996:312; 3–4.
3. Culver, J.D., Gerr, F., Frumkin, H. Medical information on the Internet —a study of an electronic bulletin board. J Gen Intern Med 1997;12:486–470.
4. Dick, R.S., and Steen, E.B., eds. The Computer-based Patient Record: An Essential Technology for Health Care. National Academy Press, Washington, D.C. 1991.
5. Elder, N.C., Gillcrist, A., Minz, R. Use of alternative health care by family practice patients. Archives of Family Medicine 1997;6:181–184.
6. Gleick, E. Picking a health plan: a how-to-guide. Time January 22, 1996:60–61.
7. Harris, E.D. Electronic mail—a physician extender? Western Journal of Medicine 1997;166:123–125.
8. Impicciatore, P., Pandolfini, C., Casella, N., Bonati, M. Reliability of health information for the public on the World Wide Web: systematic survey of advice on managing fever in children at home. BMJ 1997: 314; 1875–1881.
9. Kane, B., Zands, D.Z. Guidelines for the clinical use of electronic mail with patients. JAMIA 1998;5:104–11.
10. Kassirer, J.P. The next transformation in the delivery of health care. NEJM 1995:332–52–54
11. Neill, R.A., Mainous, A.G., Clark, J.R., Hagen, M.D. The utility of electronic mail as a medium for patient-physician communication. Arch Fam Med 1994;3:268–271.
12. Pealer, L.N., Dorman, S.M. Evaluating health-related web sites. J School Health 1997;67:232–235.
13. Silberg, W.M., Lundberg, G.D., Musacchio, R.A. Assessing, controlling, and assuring the quality of medical information on the Internet. JAMA 1997;277: 1244–1245.
14. Smith, R. The future of health care systems. BMJ 1997; 314:1495–6.
15. Sonnenberg, F.A. Health information on the Internet. Arch Intern Med 1997;157:151–152.
16. Spigelblatt, L., Laine-Ammara, G., Pless, B., Guyver, A. The use of alternative medicine by children. Pediatrics 1994:94:811–814.
17. Spooner, S.A. The pediatric Internet. Pediatrics 1996:98 1185–1192.
18. Widman, L.E., Tong, D.A. Requests for medical advice from patients and families to health care providers who publish on the World Wide Web. Arch Int Med 1997;157:209–212.
19. Wyatt, J.C. Commentary: measuring quality and impact of the World Wide Web. BMJ 1997;314:1879–1881.

Chairman THOMAS. Thank you very much, Doctor. And I will acknowledge I am the one who borrowed the information from your written statement to talk about the preventive aspects.

Ms. Goldman.

STATEMENT OF JANLORI GOLDMAN, DIRECTOR, HEALTH PRIVACY PROJECT, INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY, GEORGETOWN UNIVERSITY

Ms. GOLDMAN. Good morning, and thank you very much for the opportunity to testify here today. I am very pleased the Subcommittee is focusing on this issue and prepared to move ahead, as Congress now has set a time limit on itself.

One of the questions that was asked earlier about existing privacy laws I think is an important one as we view this in the context that we do have an existing body of privacy statutes. And while they are not terribly consistent or related to each other, in

some ways they do bear, I think, certain commonalities. I would hope that when we look at crafting a medical privacy law, we try to put it within the context of those existing privacy laws and, as you said, to learn something from what we have already done.

What Congress has recognized is that medical privacy is a critical issue and we need to move forward within a certain period of time to pass legislation, and that if we are not able to do that, if we are not able in this body to reach some kind of consensus and move forward, the Secretary will then handle this as a regulatory matter. I do think Congress has a greater role in terms of setting enforceable rules and having remedies and enforcement mechanisms in place. We do have an important opportunity to do that work here.

We have seen a much greater urgency in this area, even in just this past year. The recent stories involving the disclosures by CVS and Giant, I am sure many of you saw reported in the papers in the last few weeks, showed we are dealing in an unregulated environment. There is not now an existing Federal law protecting people's medical records.

So while people are not necessarily acting with malice, there are considerations that are being given when information is disclosed that are not patient-focused, that are not focused on what is best for the patient or that do not directly involve the patient. So the response on the part of the public to those disclosures by CVS and Giant was very swift, very angry, and in fact both of those companies took out ads in the Post to say that they were stopping the practice altogether. Not trying to fix it, but stopping it all together until they could recoup some public confidence and decide how, if at all, they could move forward with compliance and marketing programs.

One of the things I would like to suggest here this morning is that the way we have looked at privacy in the last decade in this area has been to view it in conflict with achieving public health goals. So that when we talk about privacy, we often talk about the costs associated or we see it as a barrier to getting access to data for research purposes or public health purposes. I do not think that has been a useful formulation, and I do not think it is an accurate formulation; such a view keeps us from developing the consensus we need.

One of the things I found is that exactly the opposite is true. Privacy is not a barrier to achieving public health purposes, public health initiatives, and improving access to data for research. In fact, it is the opposite. Privacy is necessary for getting good quality data, complete data, and accurate data for use for those public health purposes.

I want to spell out a few of those areas. When people do not trust that when they go to their doctor the information they are sharing will be handled in a confidential way, they do start to engage in certain privacy protective behaviors which have some very serious consequences. It has serious consequences for the individual, because if they do not accurately and fully share information, the doctor then does not have data he or she needs to accurately diagnose, to accurately treat. So the patient's care is undermined right there in the doctor's office.

But, also, doctors then are not transmitting accurate and complete data on claims forms, the encounter data that the insurance industry relies on in doing the outcomes analysis that researchers rely on in doing their studies, that public health officials rely on in doing their studies and creating population data bases. So when we do not protect the information at the front end, it is undermined at the back end. We need this accurate and complete data. And I would say we need to give people some assurance that the data will be protected so that they will fully share information.

One of the things we have seen is that the health care environment is changing so dramatically. There was an editorial in Sunday's Post that talked about privacy being a moving target and that the industry is developing so quickly, so rapidly around information uses and yet there are no enforceable rules in place. What I want to do is suggest that there are some key principles that can be built into a health privacy proposal.

We do not have unanimity amongst all of us as to exactly how that language should be written, but I want to suggest that there are some key principles on which we do agree that we need to address. One is the very basic issue of giving people access to their own medical records, a fundamental right which only half the States in this country currently protect.

We need to have limits on disclosure. We need to be able to say what information should be disclosed, how individuals make meaningful, informed voluntary choices by giving them notice of how information might be used, and having them sign authorization forms.

Research, I think, is a tough area, as Dr. Detmer has said. One of the things that is important to acknowledge is that we do have Federal rules in place right now that apply to federally funded researchers, and those rules require an institutional review board to look at informed consent, to look at when there is an appropriate waiver of informed consent, if identifiable data is to be used, and I would suggest we take those Federal regulations and apply them across the board. There would be fairness and uniformity, and all researchers, not just those receiving Federal funds, should have to comply with those regulations.

The Minnesota law is a source of some concern for folks. And while I agree it is the most restrictive law in this area, there have been studies done by the Mayo Clinic that show where consent is asked by patients for identifiable data, only 4.5 percent, on an average of people who are asked, decline. Four and a half percent of the people withhold their permission for use of the information.

Law enforcement. We need to have rules on government access to individual data. Right now every privacy law that exists on the books has a law enforcement limitation, and that is required by constitutional principle. It is the right thing to do.

Remedies. We need to have strong remedies and enforcement mechanisms.

I want to address the issue of preemption. I know it is on people's minds. We are dealing in a difficult area, because if we look at precedents of privacy laws, we currently do not ever preempt law in the civil rights and civil liberties area. In fact, Congress has been concerned about preempting State laws.

In the medical privacy law, we have a particular problem in that we do not know what laws we would be preempting. There does not yet exist a comprehensive survey of existing State privacy laws. They are located in all different areas of the State code, from public health to consumer protection to insurance regulation.

We need to have a better handle on what we would be preempting, and we need to look at whether we can determine preemption on a case-by-case basis, look at particular issues, and whether there is a justification for a carve-out in those areas. Right now there is compliance with existing State laws, so people are functioning in this environment even though it may not always be the most convenient.

Let me quickly mention some of the other issues.

Discrimination. We have an opportunity in crafting a privacy law to in some ways create the first line of defense against discrimination. We have the Americans With Disabilities Act, but nothing in that law prohibits an employer from getting access to the health information. A privacy law would do that. So it would prevent, in some ways, the temptation for using that information for discrimination.

The technology is a critical issue you have all talked about. We have a chance with the increased technology to better protect information, to create more security for data, and to recognize that paper records are essentially a fairly unprotected realm. If we need it, we can take advantage of the security opportunities we have.

And, overall, any health privacy law should create incentives to use nonidentifiable data. We should ask the question which we do not now ask: Do we need identifiable data in a particular project? Can we get by with nonidentifiable data? And by creating those incentives, we would take certain people out of the scope of the law and remove the concern.

I know this is not an easy challenge. We have worked on this issue for a long time, but I think we now have the increased political will to move forward.

At bottom, Americans should not have to worry when they go to the doctor, fill a prescription, file a claim form, or they get a job and do a preemployment physical; they should not have to worry their privacy is going to be put at risk. They should be able to fully share information with their doctors and not worry they are going to have their care threatened or their employment threatened.

We will know that we have really made some progress here when we protect our medical records as well as we protect our video rental lists.

Thank you very much.

[The prepared statement follows:]

Statement of Janlori Goldman, Director, Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University

I. INTRODUCTION AND OVERVIEW

Mr. Chairman and Members of the House Ways and Means' Subcommittee on Health: I very much appreciate the invitation to testify before you today on patient confidentiality.

In December 1997, I launched the Health Privacy Project at the Institute for Health Care Research and Policy at Georgetown University Medical Center. Prior to creating the Project, I have focused on privacy and technology issues—particu-

larly health privacy—for over a decade, as co-founder and Deputy Director of the Center for Democracy and Technology, and as Director of the Privacy and Technology Project of the American Civil Liberties Union.

At present, there is no comprehensive federal law to protect the privacy of peoples' health records. However, most people mistakenly believe there is a federal privacy law that safeguards their medical records, and they believe the law gives them the right to access their own medical records; they are shocked when informed otherwise (Louis Harris & Associates, Health Information Privacy Survey, 1993). The recent debacle involving CVS and Giant Food selling customer prescription data to drug manufacturers for target-marketing and customer tracking—and the public outrage expressed over this practice—is another loud and clear call for Congress to enact a strong health privacy law to protect people against such unauthorized use and abuse of their personal medical records.

I believe health privacy is one of the most important health issues facing our nation: it is critical to improving health care, and fostering valuable public health initiatives. Fortunately, Congress recognized the urgent need for enforceable health privacy rules, and set itself a time limit in the Health Insurance Portability and Accountability Act of 1996 to pass health privacy legislation by August 1999.

There are a number of proposals before the House and Senate with regard to medical privacy. Representative Jim McDermott (D–WA) and Representative Gary Condit (D–CA) have both reintroduced their bills from last Congress without significant change: "Medical Privacy in the Age of New Technologies Act of 1997" (H.R. 1815) and the "Fair Health Information Practices Act of 1997" (H.R. 52), respectively. In the Senate, under consideration are: "The Medical Information Protection Act of 1998," (discussion draft 2/19/98) co-authored by Senator Robert Bennett (R–UT) and Senator James Jeffords (R–VT), and "The Medical Information Privacy and Security Act," (S. 1368) introduced by Senator Patrick Leahy (D–VT) and Senator Edward Kennedy (D–MA). Last week President Clinton released the Administration's proposal for a patients' "Bill of Rights," which includes a broad confidentiality provision.

There is a long history of congressional efforts to craft health privacy legislation, but, as yet, we have fallen short of achieving the necessary consensus. I believe we must take the critical next step to move away from viewing privacy and health initiatives as values in conflict, and towards viewing privacy as a key element in ensuring the success of health care goals. In my statement, I outline a new framework for addressing privacy in the larger health care arena as an ultimate good, which will foster patient trust and confidence in the doctor/patient relationship, and enhance the quality of patient data needed for improving patient care, research, and public health initiatives.

II. The Value of Privacy to Individuals and Communities

The potential benefits to individuals and communities from the emerging global information infrastructure are well documented. More and more, people are communicating, receiving information, and engaging in commerce through the Internet, often with little regard for local and national borders. Individuals, governments, libraries, universities, hospitals, museums, corporations, and non-profits are expanding their activities to include the use of the Internet and other interactive communications technologies.

But there is a darker side to the "Information Age" that threatens to undercut the growth and promise of these powerful new developments. The same medium that makes possible the instant global communication and sharing of information, also provides people with the capacity to generate, capture, store, and reuse a tremendous amount of personal information. On a daily basis, applying for a driver's license, seeking credit, talking with a doctor, passing through a toll on the turnpike, making (or receiving) a phone call, subscribing to a magazine or joining an organization, logging on to a website, or even buying a small item with cash, often requires that people divulge a tremendous amount of detailed, sensitive information.

The primary issue here is not the use of the person's information for the purpose for which it was collected (evaluating credit, issuing a driver's license, providing medical care), but the unanticipated, secondary disclosures of the person's information. Over the course of a person's lifetime, the record of one's life collected through distributed and largely unregulated networks can make real the "womb-to-tomb dossier" that Harvard Professor Arthur Miller warned of over thirty years ago. Once personal information is collected for one purpose, the temptation to use it for other purposes is often irresistible.

In a joint statement last year, President Clinton and Vice-President Gore acknowledged the public's fear of losing privacy: "Americans treasure privacy, linking

it to our concept of personal freedom and well-being. Unfortunately, the [Global Information Infrastructure's] great promise that it facilitates the collection, re-use, and instantaneous transmission of information can, if not managed carefully, diminish personal privacy. It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business.''

Significant social, political, and economic consequences can result from our society's failure to preserve privacy. If people continue to lose control over their ability to choose when, what, and to whom to divulge personal, sensitive information, they will be reluctant and unwilling to step forward and fully participate in society, fearing unwanted exposure, judgements, discrimination, surveillance, stigma, and loss of jobs, credit, housing, or family. A continued failure to protect the privacy of personal information in a variety of spheres—most notably health—will undermine peoples' ability to fully participate in social, political, and commercial activities.

III. Privacy and Health Care

A lot of attention has been paid in recent years to how to improve health care in this country, but a critical element that is often overlooked and misunderstood is the role privacy and confidentiality plays in the health care setting. Nearly every facet of health care—from health care delivery, to payment, prescribing medication, outcomes analysis, research, and marketing—is undergoing dramatic changes as our society moves towards managed care and the development of integrated health data networks. As a recent editorial in The New York Times observed, ''Preserving privacy in the ever-expanding world of electronic medical records is a daunting task that health care organizations and public policy makers have been slow to address. But as managed care puts more information into more hands, consumer anxiety over confidentiality makes the issue unavoidable.''

A number of factors lead to privacy being viewed by some as being in conflict with other health care endeavors. These factors range from fear that addressing privacy at the patient level will lead to a diminution in the quality and quantity of health data made available, to concern about a lack of knowledge and tools to apply in protecting personal health information in both electronic and paper form. Anxiety exists among some downstream users of health information that protecting patient privacy means people will always choose to lock up their medical records in their doctors' offices.

Some of those who fear privacy will reduce the flow of valuable patient data claim that:

- There is an overriding public interest in furthering their activities which trumps any individual privacy claim;
- People will not be able to responsibly exercise any decision-making authority over their own information—in other words, they will not understand (or care about) the larger social good to be gained by the use of their information;
- There are no horror stories of improper use or disclosure of personal medical information for which they are responsible;
- The complexity and cost of putting privacy and security safeguards in place are too burdensome, and will choke the flow of identifiable health data needed for health care-related initiatives.

At bottom, some health care organizations are concerned that health privacy regulation will go too far on the confidentiality side, and thus have a negative impact on beneficial health efforts. There is a fear that protecting privacy will clog the free flow of health information, and make less information available for outcomes analysis, research, public health activities, and other health-related purposes.

Ultimately, the converse is true: without trust that the personal, sensitive information they share with their doctors will be handled with some degree of confidentiality, patients will not fully participate in their own health care. In the absence of such trust, patients will be reticent to accurately and honestly disclose personal information, or they may avoid seeking care altogether for fear of suffering negative consequences, such as embarrassment, stigma, and discrimination. Along the continuum, if doctors and other health care providers are receiving incomplete, inaccurate information from patients, the data they disclose for payment, research, public health reporting, outcomes analysis, and other purposes, will carry the same vulnerabilities.

Initiatives to improve public health and reshape health care—such as community health information networks, managed care, telemedicine, outcomes analysis, disease management, the creation of population data bases—could not exist, let alone flourish, without access to complete and reliable information. However, the current lack of privacy and security protections for personal health information threatens to undermine significantly the quality of care people receive, as well as the accuracy

and reliability of the information being collected and used for outcomes analysis, cost effectiveness studies, research, and public health activities.

I urge that we abandon the current dialogue that places privacy and public health initiatives in conflict. A new framework is needed that intertwines the values of protecting patient privacy and fostering health care initiatives. At this juncture, let us treat patient privacy as a "first principle" of ensuring quality of care for individuals and their communities. Ideally, within such a health privacy framework, identifiable information patients choose to disclose outside the four walls of their doctor's offices would be more accurate and complete, and thus create more reliable data for use by doctors, researchers, and others working to enhance the quality of health care. By expanding our focus to incorporate privacy as an ultimate good to be achieved in the health care arena, we may better advance our health care initiatives.

IV. The Role of Privacy in Care and Research

Again, without trust that the personal, sensitive information they share with their doctors will be handled with some degree of confidentiality, people will not fully participate in their own health care. In turn, information that lacks integrity at the front-end will lack integrity and reliability as it moves through the health care information environment. Therefore, protecting privacy must be an integral part of both ensuring good health care to individuals and improving the health of the larger community. If people worry that their most sensitive information will not be treated confidentially by their doctors, and may be disclosed without their knowledge and permission to their employers, pharmaceutical companies, or marketers, these people are likely to engage in privacy-protective behavior, such as withholding information from their doctors, paying out-of-pocket for services to which they are entitled or avoiding health care altogether. Anxiety on the patient's part over unknown and coerced uses and disclosures of their records—even for altruistic purposes—leads people to withdraw from full, honest participation in their care. This privacy-protective behavior serves to both jeopardize peoples' health care, as well as undermine the health care initiatives that rely on high-quality information.

In many ways, the relationship between people and their doctors bears the greatest burden in the health privacy debate; this relationship is the "hot spot," the originating point on the health information continuum. Patients are beginning to understand that the open-ended waivers for disclosure they sign as a condition of receiving health care and reimbursement for services leave them vulnerable to a wide array of uses and reuses of their health information. It is here, in the first and subsequent encounters with a particular provider, that a person decides how much to divulge, and whether that provider can be trusted. There are many factors that affect a person's trust and confidence in his or her doctors, and it is that level of trust that ultimately determines the degree of willingness to fully divulge health and other personal information.

The public has consistently expressed a high degree of concern over the vulnerability of their privacy, in particular the lack of protection for their personal health information. Decades of survey research conducted by Louis Harris & Associates document a growing public concern with privacy. The 1995 Harris poll found that 82% of people were concerned about their privacy, up from 64% in 1978.

A Health Information Privacy Survey released by Harris in 1993 found that the majority of the public (56%) favored the enactment of strong comprehensive federal legislation to protect the privacy of health care information. In fact, of that majority, eighty-five percent (85%) responded that protecting the confidentiality of medical records was absolutely essential or very important to them. An overwhelming percentage wanted penalties imposed for unauthorized disclosure of medical records (96%), guaranteed access to their own records (96%), and rules regulating third-party access to personal health information.

Harris' 1996 survey elicited a disturbing public view of researcher use of medical records. Only eighteen percent (18%) of the public consider the use of patient records for medical research without prior permission to be very acceptable. Thirty-nine percent (39%) found the use somewhat acceptable. The public's comfort level increased if the information released did not identify individual patients, but one-third found it not at all acceptable for researchers to use non-identifiable health information without patient consent.

Finally, in Harris' 1995 survey, sixty percent (60%) of respondents cited instances where they refused to provide requested information. This kind of privacy-protective behavior is not unfounded. Recent reports of abuse or misuse of peoples' health information have confirmed the public's fear of misuse of personal medical information. For example:

• The chain drug store CVS, and Giant Food, recently admitted to disclosing patient prescription records to a direct mail and pharmaceutical company to track customers who don't refill prescriptions, and send them letters encouraging them to refill, and consider alterative treatments. After public outrage was expressed following media reports of this practice, both CVS and Giant agreed to halt the marketing disclosures. ("Prescription Fear, Privacy Sales," Washington Post, p. A1, 2/15/98)

• An Orlando woman recently had her doctor perform some routine tests, and received a letter weeks later from a drug company touting a treatment for her high cholesterol ("Many Can Hear What You Tell Your Doctors: Records of Patients Are Not Kept Private," Orlando Sentinel, 11/30/97, A1)

• New York Congresswoman Nydia Velasquez' confidential medical records—including details of a bout with depression and a suicide attempt—were faxed from a New York hospital to a local newspaper and television station on the eve of her 1992 primary. After overcoming the fallout from this disclosure and winning the election, Rep. Velasquez testified eloquently about her experiences before the Senate Judiciary Committee as it was considering a health privacy proposal.

• The Harvard Community Health Plan, a Boston-based HMO, admitted to maintaining detailed notes of psychotherapy sessions in computer records that were accessible by all clinical employees. Following a series of press reports describing the system, the HMO revamped its computer security practices.

• In Maryland, eight Medicaid clerks were prosecuted for selling computerized record printouts of recipients' and dependents' financial resources to sales representatives of managed care companies.

• In a recent survey, 206 respondents reported discrimination as a result of access to genetic information, culminating in loss of employment and insurance coverage, or ineligibility for benefits.

• The director of a work site health clinic operated by a large manufacturing company testified that he was frequently pressured to provide personal information about his patients to his supervisors.

• The late tennis star Arthur Ashe's positive HIV status was disclosed by a health care worker and published by a newspaper without his permission.

• Patient Direct Metromail advertises in a pharmaceutical industry journal that it has 7.6 million names of people suffering from allergies; 945,000 who suffer from bladder-control problems; and 558,000 who suffer from yeast infections. ("Medical Privacy is Eroding, Physicians and Patients Declare," San Diego Union-Tribune, 2/21/98,

Focusing specifically on mental health care, a New York Times Magazine article, "Keeping Secrets," observed: "[A]t present it is unrealistic for people to assume that the raw and tender subjects they talk over with their therapists will go no further than the four walls of the consulting room. And many patients have become legitimately concerned about the possibility that the depression, suicide attempt, marital problem or alcoholism being discussed could return to haunt them in cyberspace. They are uncomfortably aware of the shadowy figures sitting in on their therapy sessions: the insurance administrator, the electronic file clerk, the case reviewer, other physicians with an H.M.O.—even their own co-workers and supervisors." (June 16, 1996, p. 38)

Peoples' anxiety over whether they will maintain some decision-making authority over the use and disclosure of their personal health information by their doctors strongly drives their decisions to seek care, how honestly and fully they interact with their health care provider, whether they 'doctor hop' to avoid having all of their health information entrusted to one provider, and whether they pay out-of-pocket or file a claim. Any lack of trust or confidence in the doctor/patient relationship carries the potential of infecting all of a person's interactions with and perceptions of the health care environment.

The consequences for patients, as well as the health care initiatives intended to serve them, are significant:

• The patient may receive poor quality of care, risking untreated and undetected health conditions.

• The doctor's abilities to diagnose and treat accurately are jeopardized by a lack of complete and reliable information from the patient.

• The integrity of the data flowing out of the doctor's office is undermined. The information the patient provides, as well as the resulting treatment and diagnosis, may be incomplete and inaccurate, and not fully representative of the patient's care or health status.

• A doctor may skew diagnosis or treatment codes on claim forms, or the doctor may keep separate records to be maintained and kept within the doctor's four walls, and send on incomplete information for claims processing in order to encourage a patient to more fully communicate.

• The credibility of any research or analysis performed in reliance on the patient's data is called into question. Not only is the patient's health data unreliable from her medical record and claims data, the downstream user (researcher, public health official) lacks any information as to whether the information might lack integrity or why. In other words, there may be no clue in the record that something is missing or false.

In the health care setting, when patients withhold information or shun care to protect their privacy, they must do so with a broad, undiscriminating brush—they have to calculate for every negative possibility. But, if people are assured that their health information will be safeguarded, and if they are empowered to make informed, voluntary choices about the secondary use of their health information, people are likely to seek care, more fully open up to their health care providers, and make educated decisions about the disclosure and use of their personal health information.

V. Consensus for a National Health Privacy Policy

A consensus exists among the public, policymakers, and a broad spectrum of the health care field that a comprehensive health privacy policy is needed in this country. As a recent editorial in the Washington Post concluded: "Of all the threats posed to personal privacy by new information technologies, the threat to the privacy of medical records is by the far the most urgent." ("Medical Files, or Fishbowls?" 9/23/97, p. A16)

Reports of the last twenty years are unanimous in concluding that a comprehensive national health privacy law is critical to ensuring both the integrity of the doctor/patient relationship and the continued development of this nation's health care system (See For The Record: Protecting Electronic Health Information, National Research Council, 1997; Health Data in the Information Age: Use, Disclosure and Privacy, National Academy of Science, Institute of Medicine, 1994; Protecting Privacy in Computerized Medical Information, Office of Technology Assessment, 1993). In the past few years, every witness that has testified before the U.S. Congress has stated that a comprehensive federal privacy law is critical to preserving peoples' trust in their doctors and in the health care system.

Most recently, the Presidential Advisory Commission on Consumer Protection and Quality in the Health Care Industry issued its recommendations for a patients' "Bill of Rights," which states: "individual patients' medical records should be treated confidentially, and disclosed only in order to treat them and pay bills."

S. 1360, The Medical Records Confidentiality Act of 1996 introduced last Congress by Senators Bennett and Leahy, quickly garnered broad bi-partisan support, including co-sponsorship by Senators Dole, Daschle, Kassebaum, Kennedy, Jeffords, and Frist. Despite this powerful hand holding, agreement on the scope and implementation of a national health privacy policy continues to present a challenge.

We now have a new and promising opportunity for meeting this challenge. The recently enacted Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes a provision mandating that either Congress or the Secretary of HHS establish an enforceable privacy regime to protect personally identifiable health information. (P.L. 104–191, also known as Kassebaum-Kennedy) In HIPAA, Congress set itself a time limit of August, 1999 for enacting a health privacy law. If Congress fails to act by that time, the Secretary of HHS is required to promulgate health privacy regulations by January, 2000.

To provide some guidance for legislation, HIPAA required the Secretary to submit to Congress her blueprint for health privacy legislation. In September 1997, Secretary Shalala issued a set of recommendations to Congress to "enact national standards that provide fundamental privacy rights for patients and define responsibilities for those who serve them." The Secretary's recommendations parallel to a large extent the recommendations of other national bodies, as well as incorporating approaches taken by many of the proposed medical confidentiality bills introduced in Congress over the past. The major recommendations are to:

• Impose new restrictions on those who pay and provide for care, as well as those who receive information from them. It should prohibit disclosure of patient-identifiable information except as authorized by the patient or as explicitly permitted by the legislation. Disclosures of identifiable information should be limited to the amount necessary to accomplish the purpose of the disclosure, and should be used within an organization only for the purposes for which the information was collected.

• Provide consumers with significant new rights to be informed about how their health information will be used and who has seen that information. Providers and payers should be required to advise patients in writing of their information prac-

tices. Patients should be able to see and get copies of their records, and propose corrections. A history of disclosures should be maintained by providers and payers, and be made accessible to patients.

- Provide for punishment for those who misuse personal health information and redress for people who are harmed by its misuse. There should be criminal penalties for obtaining health information under false pretenses, and for knowingly disclosing or using medical information in violation of the Federal privacy law. Individuals whose rights under the law have been violated should be permitted to bring an action for damages and equitable relief.

Secretary Shalala concludes that "without safeguards to assure that obtaining health care will not endanger our privacy, public distrust could turn the clock back on progress in our entire health care system." (Shalala report, pp 1,2.)

However, the Secretary's report drew fire from the Hill, the media, health care providers, and health privacy experts for her recommendation that law enforcement officials continue to have virtually unfettered access to personal health records. As The New York Times editorial decried: "The exemption for law enforcement agencies is a huge loophole The need to combat fraud in the nation's trillion-dollar healthcare industry is indisputable. But it hardly justifies granting less privacy protection to the intimate information contained in medical records than existing Federal statutes now extend to the records of banks, cable television, video rental stores, or E-mail users, as the Administration's plan bizarrely contemplates." (See "Trifling with Medical Privacy," NY Times, 9/97)

No other federal privacy statute provides such an exemption for law enforcement. In fact, most of the U.S. privacy laws were enacted specifically to bring law enforcement under a Fourth Amendment warrant mandate.

It is also worth noting that HIPAA includes a provision known as "Administrative Simplification." Coupled with the law's privacy mandate is a requirement that uniform health data standards for the electronic transmission of personal health data be developed by Spring 1998. The consequence of these dual and staggered requirements is that a time line has been established by which data standards must be created prior to the development of privacy and security rules governing personal health information. Both the short time frame and the awkward sequence of events laid out in the "Administrative Simplification" section pose unique challenges for health care entities, policymakers, and patients.

However, the congressionally mandated time limit to pass health privacy legislation by August 1999 shifts the political landscape, and injects greater immediacy into the effort to find a strong, workable privacy solution.

VI. Key Issues for Federal Health Privacy Policy

The following is a broad outline of the key elements that must be incorporated in a comprehensive health privacy policy. Many of the health privacy proposals currently pending before Congress address, in various ways, these key factors.

- Access: People must have the right to see, copy, and supplement their own medical records. Only 28 states currently provide such a right.
- Notice: People must be given written, easy-to-understand notice of how their health information will be used and by whom. Only with such notice can people make informed, meaningful choices about uses and disclosures of their health information.
- Consent: As a general rule, patient consent should be obtained prior to disclosure of personal health information by doctors, health plans, employers, and other health care entities, especially if the disclosure is not related to treatment or payment. There seems to be a broad recognition that exceptions to the rule of consent are needed for certain public health disclosures and in emergency circumstances.
- Research: A federal privacy law should strengthen and expand the reach of existing privacy safeguards for identifiable health information used by researchers. Overall, a national health privacy policy should create incentives for researchers to use non-personally identifiable health data.

Specifically, there should be equity, uniformity, accountability and oversight in scope and application of the federal regulations governing Human Subjects research and the use of personally identifiable health information by researchers. Regulations should be applied to both federally and non-federally funded researchers, and the existing standard for granting waivers of informed consent for use of identifiable data should be codified, strengthened and strictly applied.

Far from hindering research, a federal health privacy law can benefit health research—by bolstering patient confidence in the use of personal health information. Again, protecting patient privacy can help to insure the integrity of the data at the front end, when it is divulged by the patient.

• Security: It is important to require the development of security safeguards for the use and disclosure of personal health information. While it is critical to acknowledge that networked health information systems can pose a risk of greater magnitude and harm, technology can be used to better safeguard personal health information in electronic form than it would be protected if on a piece of paper in a file drawer (see For the Record: Protecting Electronic Health Information, National Research Council, 1997). Also, technology can be used to more efficiently anonymize and de-identify personal health data for public health initiatives.

No system—either paper or electronic—can provide 100% fool-proof security, but existing technology does provide us with some powerful opportunities to better protect personal information. There has been some discussion about providing people the option to prohibit their personal health data from being maintained and transmitted in electronic format. I believe that such an "opt-out" may create a false expectation that sensitive information is better protected in paper form. Again, this is not necessarily true if strong security policies and tools are built-in to information systems.

• Law Enforcement: A federal health privacy law should include a court order requirement, with a standard as stringent if not more so than that set out in the Video Privacy Protection Act (better known as "The Bork Bill"). Constitutional principle requires that individuals should be shielded from unjustified government intrusion. Currently, no federal privacy statute provides a broad exemption for law enforcement. In fact, most of the U.S. privacy laws were enacted specifically to bring law enforcement under a Fourth Amendment warrant mandate.

• Remedies: In order to be truly effective, a federal health privacy law must have strong remedies in place. For instance, strict civil penalties and criminal sanctions should be imposed for violations of the law, and individuals should have a private right of action against those who mishandle their personal medical information.

• Preemption: No precedent exists in our federal privacy and civil rights laws for preempting state law. In the case of health privacy, we do not yet have a comprehensive survey of state law that would even indicate what state laws we would be preempting. Further, health care entities are currently doing business and transferring information interstate, complying with various state health privacy laws.

Serious consideration should be given to any proposal to preempt state law in this area, thereby locking the states out of tailoring their laws to reflect particular circumstances. For instance, stronger state mental health and communicable disease confidentiality laws should not be preempted, given the long history of stigma and discrimination against people with these conditions. Moreover, given what we know of the resistance to testing and accessing treatment, these state privacy laws help to promote broad public health interests.

VII. Conclusion

I am optimistic that the political will exists this Congress to pass legislation that truly protects peoples' privacy in the health care setting, without unduly compromising valuable health care initiatives. The time has come for a cohesive, forward-thinking health privacy paradigm that acknowledges privacy's critical role in health care, and integrates it at various states throughout the health care system. People must be empowered to be more active, informed consumers of health care and knowing, willing participants in the broader health care activities that impact their lives and well-being of their communities. If we are to achieve the oft-touted goals in health care, people must have trust and confidence that the health care system will safeguard their personal health information. Loss of personal privacy—and ultimately the erosion of reliable health information—must not be the price of progress.

Chairman Thomas. Thank you very much.
Dr. Birge.

STATEMENT OF JAMES BIRGE, M.D., MEDICAL DIRECTOR AND CHIEF EXECUTIVE OFFICER, MACGREGOR MEDICAL ASSOCIATION, HOUSTON, TEXAS; ACCOMPANIED BY JIM SLOANE, VICE PRESIDENT OF BUSINESS DEVELOPMENT, AMERICAN MEDICAL MANAGEMENT, HOUSTON, TEXAS

Dr. BIRGE. Again, thank you for inviting us to testify here. I am Dr. Birge, the medical director and the chief executive officer for MacGregor Medical Association. With me is Jim Sloane, vice president of business development for our computer systems. We are here to describe what we have been doing with electronic medical records from a clinical standpoint, which I will address, and Mr. Sloane will address it from a security standpoint with a little show-and-tell of what it looks like.

Essentially, I echo everything that Dr. Borowitz said in his testimony. MacGregor is a fairly large group. Right now there are 22 sites in Houston, 5 in San Antonio, a total of about 220 doctors. We are taking care of about 210,000 patients in Houston, about 40,000 in San Antonio. By the end of the eighties it was very apparent to us that the paper medical record just did not work. We could not get the clinical information to the doctors at the time the doctor needed it. The only answer we came up with was the computer, and that is what we did.

We installed an electronic medical record that went live at the end of 1991, and all of the patients are now in that computer base. It handles 1.1 million visits a year. It makes available essentially all the outpatient data for the physician at the time the physician needs it. We do this by providing computers in the doctors' offices, nurses' stations, in the ERs of plan hospitals, L&D, that sort of thing. They can also have access at home, if the physician wants.

What that does is allow us to use the computerized information, which includes progress notes, lab reports, x rays, and problem lists, and use it in four fundamental categories: The first would be taking care of that individual patient, so that whether the patient shows up at the office on a scheduled visit, or they are showing up in the evening as a walk-in; or they are hitting the L&D room or the ER of the plan hospital, the medical information is there for the physician taking care of the patient. As other people have previously testified, the quality of care is better that way, and hopefully things are more economical and expedient from a time standpoint.

A quick example. A 70-year-old woman hits her after-hours facility; feels a little tired, a little dizzy. The doctor does a review—does not have the paper record available but does have access to the clinical information in the computer. Finds a hemoglobin at 10.1, which is slightly anemic. Is that new or old? Should he worry or not worry? The computer says the hemoglobin has been like that for the last 10 years. You are not going to worry about it. There are just numerous examples like that.

Second point: Identification of high risk patients. The medical paradigm, if you allow me to use this trite word, has always been episodic. We wait for the patient to intervene with us. We wait for them to get sick, feel lousy, something bad is happening, and then the doctor jumps in and tries to save the day, usually with poor success.

What we need to do is move to the next millennium, and that is identifying the high risk patients before they blow up. How do you do it? Information. The computer systems can look at patients with mild renal failure. They have not been back in to see a doctor in more than 1 year. That is a high risk patient. Somebody whose glucose is not under tight control, hasn't seen a doctor in 6 months, that is a high risk patient.

This is where the medical profession needs to go. It is our obligation to take that next step, to treat the patient as a continuum, not as an episode, and that all requires information linked together chronologically.

The third area is quality assurance just within our organization. This would be data which is really not identifiable by the individual but looks at all the conditions of how tightly controlled are diabetics, what kind of renal functions are they obtaining, that sort of thing. This comes back to the outcome analysis the Chairman talked about earlier.

And then, finally, quality assurance, or outside our organization; these are HEBIS initiatives; NCQA, that sort of thing, again where you can screen computer data as opposed to hordes of nurses floating through paper records one by one. It is a no-brainer. Obviously, the results are going to be more meaningful from a statistical basis, and you can look for more things using the computer than you can the paper record.

With that, let me turn things over to Jim Sloane.

Mr. SLOANE. Good morning. Thank you for the opportunity. I would request that I move my seat over, and hopefully my technology will work appropriately and I will demonstrate some of what the providers at MacGregor have access to in our information system.

To start off with, in addition to the confidentiality statement which every employee must sign as a condition of employment, every time that one of the users turns on their PC, this is the statement that they are presented with. The only option they have, in order to continue to use the PC in any manner, is to agree with this confidentiality statement. It serves as a constant reminder to the employees about the importance of keeping the patient information confidential.

Chairman THOMAS. I do not want to interrupt you, but what is the consequence of violating that statement? I am trying to—immediate dismissal?

Mr. SLOANE. Correct.

Chairman THOMAS. Is that a right that has been exercised?

Mr. SLOANE. It has.

Dr. BIRGE. You are right, the consequence is immediate termination.

Chairman THOMAS. And it has been exercised?

Dr. BIRGE. It has been.

Chairman THOMAS. OK.

Mr. SLOANE. The step for the user when they attempt to access the electronic medical record system is the same as many other systems. Each user has a unique identifier, user I.D., to gain access to the system. They also have a password. We do force the users to routinely change their passwords so that they cannot consist-

ently use the same password. We also do not allow reuse of the passwords, so that they cannot bounce back and forth between one and two passwords.

These screens do have automatic timeout after certain periods of inactivity and the user is logged off.

Once they sign on to the system, depending upon the level of access, and it is different depending upon what type of position an employee has with the organization, they are presented with a menu of icons which they can choose from. Many of the providers start out with this view. It is basically a look at their schedule; what it looks like for a given day and a given month of the year.

From this particular view, the physician can select a patient record off of the scheduling system and start looking at clinical data. This information is similar to what we just saw, just presented in a different format. The physicians have access to laboratory results, transcriptions, immunization histories, demographic information, and significant problems, as well as drug allergies.

In order to look at a particular note, the user would just select which note they wanted to see off the appropriate tab. This happens to be my son's record. That is a common occurrence, too. This is my son's actual record from within the system. This happens to be a note dictated by Dr. Patel when my son came in for a visit. This is the immunization flow sheet.

This also serves as information for what type of immunizations were given and as a reminder to the provider when particular immunizations should be given. This is just a view of the drug history.

We have the capability within the system to search across the medical records for a given patient. In this case we search for the word "sinusitis" and the system highlights which particular progress notes contain that word or phrase. And again we see that highlighted within this progress note.

I have pulled up a different patient here. This is a test patient within our system. We see a list of the significant problems in the upper left-hand portion; on the right-hand side we would see drug allergies; and below that the same information as previously seen. If you wanted to look at a particular lab result, you can select it off the lab folder. You see the particular details of that result and then the physician has the capability of graphing the results if they desire.

This is just a different view of the same laboratory information, providing a little more detail before you go in and look at a particular result.

That is basically what I had prepared just to give you an idea of what the system looks like. But to address more specifically some of the security aspects, I already talked about the users agreeing to the confidentiality statement. We also have the capability to restrict a user's access to the system by day of the week, hour of the day, and location of the device from which they are accessing the system.

Also mentioned, we have the capability of restricting access by the level of user, so that not all users see all levels of patient information.

We do keep audit trails of access to all of the information. Every time one of those records is pulled up of a patient and you go into a progress note or a laboratory result, that information is recorded in an audit trail.

And to address the opening question, that is one circumstance where we monitor those audit trails on a routine basis. We noticed one particular employee had an unusually large number of accesses to patient records, patient data. When that employee was confronted, he immediately resigned. And we would have terminated him anyway if it was inappropriate use of the information.

We do restrict access to other employees' information within the system, so that one employee cannot pull up another employee's information unless they have a high level of security in order to do so. And that can expand beyond just other employees. Certain individuals whose records are determined should be restricted, we have that capability.

As far as the future of where we are heading, the use of a user I.D. and password is not the ideal situation. We continue to monitor the technology that is coming about. Two important areas are the use of fingerprint recognition devices, as well as retinal scanning devices. We have prototyped a fingerprint recognition device. We think it is very promising.

Obviously, a fingerprint is not something that can be shared with other people. You cannot pass it on to other people. The technology is improving and the devices are becoming much more cost effective in order to look at implementing that type of security. We think that will help tremendously.

In closing, I realize my time is up, and I would just like to state that I believe electronic records, with the appropriate controls, security, and auditing mechanisms in place, can be as secure, if not more so, than the hard copy patient records.

Thank you.

[The prepared statements follow:]

Statement of James Birge, M.D., Medical Director and Chief Executive Officer, MacGregor Medical Association, Houston, Texas; Accompanied by Jim Sloane, Vice President, Business Development, American Medical Management, Houston, Texas

Mr. Chairman, thank you for the opportunity to testify today regarding the important issue of patient confidentiality. I am Dr. James Birge, Medical Director and CEO of MacGregor Medical Association. Accompanying me today is Jim Sloane, Vice President of Business Development at American Medical Management. Jim will briefly demonstrate for you the superior security system we have developed at MacGregor. This system not only ensures patient health information is kept strictly confidential, but also enhances our ability to provide our patients with the highest quality, state-of-the-art health care available.

MacGregor Medical Association is a multispecialty clinic founded in 1953 by two physicians in Houston, Texas. It currently comprises 220 providers located at 22 sites in Houston and 5 sites in San Antonio. In Houston the physicians serve approximately 185,000 commercial HMO members, 10,000 Medicare risk enrollees, and 15,000 fee-for-service patients. In San Antonio, the operation handles 18,000 HMO paneled members and 24,000 PPO or fee-for-service patients. The total combined visits for last year were 1.1 million.

MacGregor is illustrative of the trend toward highly integrated health care systems. We have entered into a number of innovative arrangements with health plans and facilities and are responsible for several hundreds of thousands of patients. Along with this trend toward integration, however, has come new challenges over how to best keep patient information confidential while also making the information readily available for use in providing services to patients.

This is the challenge Congress now faces—how to enact standards which ensure the highest level of patient confidentiality possible without undermining the ability of health plans, physicians, and other providers to use the information for producing higher quality health care services and treatments.

Until very recently, the field of medicine has been devoted to mostly identifying and labeling various disease processes. Physicians have been able to cure almost nothing, though ameliorative treatment has made great strides over the past three decades. I believe that things are now changing. New, powerful medications and procedures entice us with the prospect of actually curing a few things and certainly controlling various disease and conditions a lot better than before. This possibility will require that a physician has prompt, complete medical data. Inadequate information will not only be costly in terms of delaying proper diagnosis and treatment, but could potentially be seriously harmful to the patient. In addition, complete medical information is necessary to conduct ongoing quality assurance activities and to continue the drive towards excellence through peer review and outcomes analysis.

For example, today's medications are far more powerful than those used 20 years ago. If a doctor doesn't know what medications a patient is taking and attempts to treat another condition, the results may be catastrophic. It is our opinion at MacGregor Medical Association that medical information must be available in the context of an electronic medical record. Not only will the industry soon demand this technology, it will be malpractice to treat a patient in the absence of complete medical information. It is therefore our challenge to create a system that:

- Uses practical industry-wide standards
- Establishes safeguards to protect patient confidentiality without jeopardizing the usefulness of the electronic medical record
- Prevents medical information from being used inappropriately
- Develops a process of funding the electronic medical record which does not unfairly affect the patient, employer, physician, insurer, or hospital.

MacGregor is a pioneer in the move toward electronic storage and transmission of patient data. MacGregor has received a great deal of national recognition and has won awards for the systems that it has developed. While this brings us a great deal of satisfaction, the more important matter is that we believe that these systems have assisted the caregivers in providing cost-effective, high quality care to the patients that they serve.

At MacGregor, patients have always been allowed to see any primary care physician at any site. As a result of this policy, MacGregor realized by the late 1980's that all too often, we were unable to deliver the paper medical record to one of our offices scattered across Houston in time for a patient visit. It was decided that the only solution was a computerized medical record. This instrument went on-line at the end of 1991 and has been successfully used ever since. In addition to the electronic medical record (EMR), MacGregor continues to use a standard paper chart which is protected by standard policies and procedures.

Through the EMR, a MacGregor physician has access to a patient's significant problem list, drug allergies, progress notes, laboratory results, X-ray results, and immunization data. This information is available at the MacGregor clinics, plan hospitals, and—if desired by the doctor—at the physician's home via the Internet.

The Structured Query Language database, which is explained in more detail in our written testimony, data base allows our physicians to perform a multitude of comparative studies which, we think, improve overall patient care. Again, without access to this data, quality of care is significantly compromised. Reports are particularly useful in identifying high-risk individuals and those patients who are overdue for screening tests. Some examples include: women overdue for mammogram; women overdue for a PAP smear; abnormal blood tests which haven't been repeated in a certain period of time; children who are due for certain immunizations; renal failure patients overdue for kidney tests; diabetics who have poor sugar control; and high cholesterol patients with inadequate follow-up.

Results of such studies are patient specific so that the clinical department may contact the patient and arrange to have the appropriate action taken.

Federal standards which either limit our access to this information, or requires that we obtain patient authorization at every point of contact, will serve only to undermine our quality control and enhancement efforts. Results of such studies are patient specific so that the clinical department may contact the patient and arrange to have the appropriate action taken.

Security of the Electronic Medical Record

In spite of the positive aspects and advantages of an electronic medical record, we are certainly aware of the potential damage and danger of this information being

disseminated to improper individuals or being used for other than the intended purpose. With that in mind, we will present the security measures and procedures that MacGregor has implemented to help prevent misuse.

We consider ourselves a pioneer in the development and use of these types of outpatient clinical systems. While this brings us a great deal of satisfaction, the more important matter is that we believe that these systems have assisted the caregivers in providing cost effective, high quality care to the patient that they serve. It is simply impossible to have a hardcopy medical record available in 30 outpatient locations, emergency rooms and labor and delivery areas of the local hospitals, all at the same time, in anticipation of a patient showing up on the doorstep.

Our central computing facility, which houses the patient clinical data, has several physical security measures in place. The front entrance to the building is monitored by a receptionist who ensures that all visitors to the building sign in and list which employee they are visiting. The receptionist then places a phone call to the employee letting them know that they have a visitor. The visitor is accompanied during his visit to our facility. The employee entrance to the building and the parking lot are secured 24 hours a day, seven days a week, 365 days a year. Each authorized employee, who has filled out the proper form, is given an access card to the parking lot and the building. Every time the card is swiped to enter the parking lot or the building, an entry is made in an electronic log which lists the owner of the card and the date and time they entered. The section of the building that houses the computer on which the data resides is also secured by an additional card reader. During off peak hours, when the employees working in this area are not present, only those select employees who have a need to enter the computer room are able to do so by swiping their card. This is also recorded in an electronic log.

With respect to the EMR application that grants users access to patient data, only those users who have filled out the proper forms, have been authorized and approved by their manager, and have been assigned a User ID and a password are able to access the system. In addition, we have software in place which mandates that users change their passwords on a predetermined basis and which prohibits reuse of passwords during certain time intervals. Additionally, to limit the possibility of an employee leaving his system logged on indefinitely, the EMR application "times out" after a period of inactivity and the user is logged off of the system. Every time that a personal computer is powered on by a user of our system, the user is presented with a confidentiality statement, a copy of which is attached, to which he must agree in order to gain access to the EMR application. This serves as a constant reminder to our employees about the confidential nature of the information contained within our system.

When remote users access our system, via direct dial-up on through the Internet, in addition to the User ID and password that are required to gain entry to the application, they must also have a second User ID and password to gain entry to the remote access server. This is in addition to a piece of proprietary software that they must have loaded on their personal computers in order to gain access remotely. All data that passes through the public network is encrypted through the use of this remote access software. We also use an Internet firewall which prevents our systems from being directly accessed through the Internet. Every outside system attempting a connection to our EMR system must first pass the criteria we have established. In our environment, the EMR is not accessed directly from the Internet. Access is first passed through a firewall and then to a gateway server that connects into the EMR system.

Through the use of internally developed security software, we also have a great deal of control over access to the EMR and other applications. We have the capability to restrict a user's access by day of the week, hour of the day, and the location of the device which he is using to access the system. We can allow or restrict an individual user's access to all, or select elements, of patient data. We can restrict access to another employees' clinical information as well as other individuals whom it is determined should have restricted access to their clinical data. Within each "window" of the application we have the ability to restrict access to any or all of the following functions: inquiry, add, update, or delete capability. Within the MacGregor Medical Association provider group, which practices in two different cities in the state of Texas, we have the ability to logically separate patient's data by region code. Although patient data is not generally made available to the doctors from the city in which they do not practice, if a patient visits the doctor in the other city and signs a release form, electronic access to the data can be granted.

In addition to all of the security measurers mentioned above, we maintain an electronic log in which a record is kept every time that a user accesses patient clinical data. This log lists the User ID that accessed the data, the date and time of the access, the type of information that was accessed, and the terminal ID from which

the access was made. This log is monitored on a regular basis by the security administrator in an attempt to determine if patient records are being accessed improperly. In one particular circumstances an employee was confronted about his unusually high number of inquiries to patient clinical data. The employee immediately resigned. While some may rightfully argue that this auditing capability is "after the fact," compare it to the inability to audit access to hardcopy patient records. While in many places a handwritten log is maintained, I would argue that it is not nearly as accurate or effective at limiting inappropriate access to patient medical records.

We know that a User ID and password mechanism is not 100% foolproof, so we continue to research and evaluate alternative means of uniquely identifying individual users of our system. Two promising possibilities include fingerprint recognition and retinal scanning. These types of systems are becoming more and more feasible as the technology improves and the cost declines.

There is a tremendous tradeoff between the level of security implemented and the usefulness and usability of any computer system. If the restrictions imposed are too severe and time consuming, the physicians and other providers will not use the system regardless of the value it brings. I believe that Electronic Medical Record systems, if implemented with the proper controls and auditing mechanisms in conjunction with enforced policies and procedures, can be made as secure, if not more so, than hardcopy medical records.

In conclusion, thank you again for the opportunity to testify on this complex and important issue. As you face the challenge of enacting federal confidentiality standards, MacGregor encourages you to reflect on the advantages of responsible use of patient information and to consider the negative consequences of imposing measures that are so restrictive that they undermine quality.

The challenge is great. The rewards for the patient and the system as a whole will be fantastic.

CONFIDENTIALITY POLICY STATEMENT

All information in a patient's medical record is STRICTLY CONFIDENTIAL. This information should not be discussed with anyone other than MEDICAL PERSONNEL with proper authorization and a LEGITIMATE 'NEED TO KNOW'. Breach of confidence may be grounds for immediate dismissal.

Chairman THOMAS. Thank you very much. A question first to Dr. Birge and you, Mr. Sloane, but Dr. Borowitz may want to respond. The software you are utilizing, is it proprietary, is it off the shelf, partially off the shelf, modified for your own use?

Dr. BIRGE. This software was developed by us, because back in the late eighties we could not find anything out there we thought would work. We would happily talk to any entity that would like to use it.

Chairman THOMAS. So, you are still amortizing the cost of development. I was going to ask whether or not you were keeping track of its cost effectiveness in terms of saving dollars for patient care. But because you had to do a bit of creating with this as well, it probably is not a fair question, because I don't think we should require the amortization of the software as part of the cost effectiveness.

Dr. BIRGE. That is a very good question. We are certainly keeping track of the expense. The system was written up in the CIO magazine and received an award a couple of years ago, and did a breakdown of some cost analysis. The real problem is what others have identified earlier, that when you start talking about being proactive and prevention therapy, that sort of thing, your payback is measured in years and decades, not quarters or one financial year. That is an issue.

Chairman THOMAS. Dr. Borowitz, is yours proprietary or created?

Dr. BOROWITZ. A hybrid of the two together. We do have some cost data regarding pharmacy errors when we brought up what is called physician order entry, where the doctors order the prescriptions themselves. And when doctors made the entry directly, the errors dropped to virtually zero within several months.

Chairman THOMAS. Well, it has obviously come to my attention this is a two-way street; that not only are you allowed to make sure you are cost effective in dealing with what needs to be done in a timely way, but that those who are not doing it in a timely way are exposed as well.

Dr. BOROWITZ. That is correct.

Chairman THOMAS. Any reaction from physicians or other health care providers about big brother looking over their shoulder in terms of making these decisions?

Dr. BIRGE. From our standpoint the answer is really no. We are a group practice, and that whole culture is one where you know people are looking at what you are doing and you are expected to be on your best behavior.

Chairman THOMAS. The concern about confidentiality. And, Ms. Goldman, although I agree with you in part, I find it difficult to talk about the points that you mentioned—discrimination, identifiable data versus encrypted paper records versus electronic and the rest, and start with the assumption that privacy is so critical and important that we ought to immediately carve out a role for States to make decisions not limited by the broader societal needs and the protection of the individual, which may, in fact, create a crazy quilt pattern that would deny us the opportunity.

I think this teeter-totter is very, very difficult to balance. My concern, and Dr. Detmer's concern, was the administration's position that States certainly should be able to go beyond what the Federal Government does in terms of rights of privacy. And I am trying to figure out where we wind up tipping in the direction of privacy which denies us, without real reason, the ability to collect data. Does that concern you at all?

Ms. GOLDMAN. Well, it absolutely concerns me, Mr. Chairman. If I can just address the preemption issue for a moment to try to respond to your concern, right now we do have this crazy quilt in the States, with nothing at the Federal level. The States are having to respond to the vacuum created by the absence of a Federal law, so they are moving forward to pass privacy legislation.

What we have seen in other areas, for instance the Federal wiretap law, is that, as all other privacy laws, it creates a floor and States are able to go beyond that. The Federal law, for instance, requires one-party consent before a conversation can be taped or intercepted. What States have done, one-third of the States, not more than that, they have decided that is not a strong enough protection and all parties must consent to the conversation. So when law enforcement goes into a particular area, they understand that that State's law must be complied with if it is above what the Federal law requires.

Now in this area I think it is a little more complicated, since we are dealing with so many.

Chairman THOMAS. You need to stand that whole argument on its head, do you not, as you are examining the issue? Does that make sense to you?

Ms. GOLDMAN. Say again.

Chairman THOMAS. The idea perhaps, where it is identifiable patient records, we can create an opportunity for States to go significantly beyond what the Federal Government believes is appropriate. But where we have protocols for encryption available, I would be very concerned about letting States go beyond the level that we establish to create that opportunity for uniformity of collection of data.

Ms. GOLDMAN. One of the ways I think we have tried, for instance, in some of the Senate proposals of last year and on this side, the way we have tried to address this concern about uniformity, because researchers and industry representatives have a valid concern, which is that it is more convenient, more efficient, often easier to transfer information around the country if you only have one standard with which to comply and you do not have to look at all the various State laws. But we have an opportunity to make that a reality without having to broadly preempt State law by making sure the Federal law is written at a high enough level.

And, in fact, many of the proposals have been written with that in mind, looking at some of the existing State laws and saying, Let us make sure we do not disregard the efforts that California has made or that New York has made, and that we make sure the Federal law is set at that level, if not a little higher, so we are not preempting State law. We allow those laws to stand and be acknowledged and respected, but we are also knowing at the Federal level we need to set the bar high enough so that there really is, in effect, one standard.

But I do acknowledge there may be some areas where we want to carve out for preemption. Research may be one of them. We may want to say that the Federal policy, as related to research, is preemptive. We may want to acknowledge, though, that in the public health area, as Dr. Detmer said, or in the mental health area, States have been fairly active, for good reason, to protect their citizens proactively in this area of crafting privacy legislation, and we should be careful not to preempt those particular laws and look at where we have a justification for preemption.

Chairman THOMAS. I do not want to get into a debate over this, but my concern there is if we deal with the use of the material itself, we may be missing the point. Rather than focusing on identifiable records versus nonidentifiable or encrypted records, the question is how good is the encryption.

Because your point about the Minnesota law, to me, is not a very valid one, and that is, Gee, we come within 95.5 percent of accuracy in some areas of collection of the data, especially in epidemiology and other areas, throw it out. It is not worth anything.

Ms. GOLDMAN. I understand.

Chairman THOMAS. The whole value of the Mayo Clinic in its approach was it was a 100-percent universe, which gave you the ability to do certain things. When you are dealing with certain types of research, especially following on our carryback, you have to have 100 percent or it is not worth anything. And to get Mayo Clinic to

spend its own money to convince people up front they should sign the waiver, which by the way is like a 60-day window and then it is gone and you have to go back and get it, is, I think, not a good model to use regardless of their ability to drive that close to 100. Because I believe there is now something being lost in Minnesota because of the Minnesota law being operative, and we will hear from someone else on the panel that may not go as far as I did.

But the other point I want to make is, I am very concerned, as we talk about the timeframe in which we are going to make laws, that we do not get too carried away with the anecdotal model for us to legislate with. The Minnesota, CVS-Giant Pharmacy list, has been used by everyone. The Maryland State legislature is moving to change that. Once it was identified and the problem was exposed, they are moving to solve the problem.

Your argument that there are people who are carrying out certain behaviors of denial in terms of the physician-patient relationship because they are worried about confidentiality may, in fact, be the case. But I have also heard enough testimony about the failure in medical school for physicians to get a little bit of training in sensitivity, that perhaps the inability of the physician to draw out the patient, to talk about this information, is a lot closer to the real world model than the patient coming in and creating a defensive posture of not telling the doctor everything because they are worried about confidentiality.

I think confidentiality models clearly would come from someone who is very concerned with privacy, but the failure of the doctor to do a good job of interviewing may, in fact, be closer to the real world. I do not want to argue the point. I want to say the anecdotal arguments are not going to be the ones we are going to legislate on, I hope. But, frankly, with the medical folk and press here, all we ever read about that makes the front page is anecdotal, and that is what our colleagues are going to respond to if we do not do a good job in trying to create a broad-based record of what the problem really is.

Now, I will give you a chance to say something.

Ms. GOLDMAN. Mr. Chairman, you make some good points, and I want to respond to the concern about the Minnesota law. I am not advocating we take the Minnesota law and make it the Federal standard. I just wanted to point out that in their——

Chairman THOMAS. I understand.

Ms. GOLDMAN [continuing]. In their efforts there is the compliance rate they have gotten. What I am suggesting is that while a 4-percent error rate may suggest to epidemiologists to throw out the data, it is worthless, and I think that is a very important point, what we have not yet measured because it is so difficult to measure, is when people are worried about confidentiality, and of course there are other factors that keep people from fully disclosing information. I recognize that. I just want to raise the point that privacy is one of those factors.

Where people do not accurately share data, where they do not fully disclose with their doctor or withhold or do not seek care at all, that undermines the quality and reliability of the data, and we have no way to measure that.

Chairman THOMAS. I understand your point. You made it well, both in written and verbal testimony. My concern is if we do not move at the Federal level, the Minnesota example will be the one used more often than not. That is my concern. And it is just not a good model, as far as I can tell. There might be better ones out there, and what we need to do is set an example.

The concern about access, and again, Ms. Goldman, you are the one who focused on this, I do believe the patient should have a right to look at their medical records. The concern I get is that the next breath leads to, We ought to be able to supplement those records, we ought to be able to add to those records, and then even to the extent we ought to be able to delete from those records.

I just want to have some statement on the record by the two doctors in front of us on this panel about their belief or attitude, in the material that they deal with, of patients being able to supplement their own medical records. I think the deletion one is a strong one. We all agree that that is not a concern. But has there been a discussion among the group or with you, in terms of the e-mail you get and about the supplementing of records?

Dr. BOROWITZ. We have certainly discussed it. I think the e-mail experience suggests that a lot of people are more comfortable writing information down, if you will, to use e-mail as a written analog. They have an opportunity to think things out without the pressure of time and being intimidated by a physician.

I also believe it is an opportunity to allow patients to short circuit some of the history-taking process, because they can present the physician or health care provider with data they may think is important but is not readily available in a written record, so that they can put their medications, their allergies, the family history, and they can get down to what is important, which is the reason they showed up in the office that day.

Chairman THOMAS. Do you think that patients withhold information purposely over the concern of confidentiality?

Dr. BOROWITZ. I have no data, but my personal experience is what you have already alluded to. There is usually another agenda that is not addressed, and it is that we have not asked the right questions to get that information; there is a fear they may not even know that we need to help them articulate. My brother's sister's uncle had appendicitis for 8 years, and you never asked me that question.

Chairman THOMAS. All I am trying to do is indicate there are a lot of reasons why it occurs, it is not just unidirectional.

Thank you very much.

Does the gentleman from Louisiana wish to inquire? Does the gentleman from California wish to inquire?

Mr. BECERRA. Dr. Borowitz, and actually Mr. Sloane and Dr. Birge as well, because you mentioned how important it might be in the future to head toward electronic data as the main source of information on patients, the question I asked earlier of Dr. Detmer is, How do you make sure you get everyone on board, if you want to make sure all patients have access to that same information and are provided the same type of health care coverage and expertise? How do you make sure the person who has to use that nonprofit, very valuable clinic in the community but is one of those that oper-

ates strictly on the margin, how do you make sure they get on board quickly?

Dr. BOROWITZ. I do not have a good answer to that question, except to say there are certainly large costs in the medical system now related to the generation of information for billing. The example I give in our own organization, which is nonprofit, is that it costs approximately $12 to collect the necessary documentation to submit the bill to the billing computer system. Those data are of no clinical value.

If we developed clinical information systems that in fact collected clinically relevant information, and as a result we had standardized billing processes, there would be a lot of money available. It would probably not solve all the problems but it would solve some of those problems. We would get more value for the systems already in place.

Dr. BIRGE. In our universe, that effect has certainly helped us. The vast majority of our revenue is by capitation. So, we are not billing, per se, to an insurer. It costs us about $7 a visit for the system you saw. So, again, the dollars saved on the billing side can be transferred over to the information side.

The other part is that we still have a paper record. It does exist. And if there would be some way to actually eliminate that, that is additional savings. It is just we have not figured out exactly how to do it.

Mr. BECERRA. I agree with everything you have said. It is just how do you make up for the startup costs? You are talking about institutions that probably have to get the computers and get the programmers and figure out how to work all of this out. How do you help them with that startup cost so they can help save money and start transitioning into that period where they are using only electronic data?

Dr. BOROWITZ. I would suggest one of the things we need to know is, How much money are they already expending on information systems that are sequestered in the billing universe?

Mr. BECERRA. But that will not end so long as they have a patient that came in and was tracked with paper records. That patient remains that way. Somehow you have to start them into this new era. You are right, as soon as they get into it, they will probably save money, but that will not help them to buy the computer to get them there.

Dr. BOROWITZ. We are in the process of upgrading our entire system throughout the University of Virginia health system, and one of the things we have realized is there is a core data set that most physicians want. It is fairly straightforward information. It is a problem list; list of allergies, list of medications, list of encounters. Those are things that can be captured fairly easily and backloaded into a system so you start with value in the system right off the bat.

When we brought up our regional immunization registry, one of the things we realized is no one would use the system unless there was information already in it. We had to go back and backload, through office charts, 2 years' worth of data. We hired a bunch of high school students to do that. You will have to have some data in the system up front for there to be value. There are core data

elements that all of us want that would provide for a lot of the needs we have.

Dr. BIRGE. I would also have two suggestions, and I think you stated it earlier, but in the for-profit sector you could do things from a tax standpoint which could be advantageous. And for both the for-profit and not-for-profit sectors, this is a plea, but the requirements of various agencies, governments, insurers are so onerous and so expensive that if you took just 20 percent of that away, there would be a lot of money left over to work with information systems.

Mr. BECERRA. OK. Let me provide, if I may, a couple of other questions that I hope can be responded to quickly. I know I do not have much time.

Mr. Sloane, you mentioned that access to information on this data base that you have is limited to level of user, or I guess you mentioned different levels, the user levels and so forth. What gives you access? At what point does someone at the hospital or this provider have access to this type of information on this data base?

Mr. SLOANE. Well, each user in the system is set up with a user profile. Typically, depending upon the type of position they have, whether or not they are a physician, a physician's assistant, a nurse practitioner, a file room clerk, or a medical assistant, we can restrict access to certain pieces of the information when we set up their profile. So that within each window of the application that you saw, we can set up every user to have either inquiry, add, update or delete capability, or no access to it. So it really is determined by the medical group, on a need-to-know basis, what level of information a particular user should have access to.

Mr. BECERRA. So the data entry person—I think Dr. Borowitz' high school students had entered data—how do you restrict access to information if you could have a data entry person be almost anyone?

Mr. SLOANE. In our circumstance we have data entry people who input information off the encounter tickets. They have absolutely no access to the clinical information system at all. There is not a need to have it, so they do not. They just cannot get into the system. Their user ID and password do not allow them access to the clinical information.

Mr. BECERRA. One final question, if I may, to anyone on the panel. As I asked Dr. Detmer, How do you protect that ultrasensitive information, the person who has AIDS or the person who has a mental history? How do you protect that, and how do you resolve the dilemma for the person who has had the information disclosed?

Ms. GOLDMAN. Well, I think one of the things Congress is trying to do is to create a standard of protection that allows people to get notice about information practices and make real choices so people can decide what is the most sensitive kind of information for them.

Some people would consider cancer-related information or mental health, genetic tests, HIV-related. Everyone has, I think, a different experience, depending upon the encounter, as to how much they want to protect it. So I think we can build some flexibility into a Federal policy that allows people to make those choices with their physicians, with their health care providers.

And the remedy piece of it, which I think you are asking about, is a very important part. We have seen some of the failure of the existing privacy laws related directly to lack of strong enforcement mechanisms or lack of strong remedies. Right now the CVS or Giant story may be anecdotal for people who felt violated by that and felt it was an inappropriate disclosure. There are very few remedies available to them.

Dr. BIRGE. I would just add that certainly it is more of a political call, I am sure, but as far as the doctor in the trenches is concerned, that doctor wants all the information that is available at that time, regardless of sensitivity, so the trick is how to do that. And I would again toss out the example you have heard, on the one side the privacy issue which is very, very important, but on the other hand you could have extremely adverse outcomes all the way up to death simply because you did not know something that you should have known, and the family is going to be very upset at that unfortunate outcome.

Mr. BECERRA. Thank you. Thank you, Mr. Chairman.

Chairman THOMAS. Of course, our ongoing concern is that we do collect that data, and it just seems to me we fought the battle on preventive care and finally won by spending the money.

Maybe we talk about rewarding those who provide us data in the usable form to move toward that outcome. They get rewarded in some way in the system, and those that do not, do not, which would get us the base level of data out there faster than would otherwise be the case.

What I find is a bit of an anomaly. You walk into a doctor's office and behind you are these shelves of individual manila folders with patient histories, but if you give them your credit card, they go to a computer and the billing is all computerized. It is the mental set of not computerizing the records because they have the hardware in the office. Perhaps we need to push software development.

But, clearly, if there was a reward for putting it in a particular form, I imagine the private sector software would be out there quickly, or some entrepreneurial doctor like Dr. Borowitz will have something on the market that has already been pretested at the University of Virginia.

But I want to thank all of you very much. This is an important area, and we are going to continue to rely on you to assist us. We do not want to legislate by anecdote and do not want to make mistakes that have to be corrected, but it is an area we will have to move in fairly quickly.

Thank you very much.

I would call today's final panel, then: Dr. Sherine Gabriel, associate professor of medicine and epidemiology at the Mayo Clinic, Rochester, Minnesota; and Dr. Harry A. Guess, who is head of the epidemiology department of the Merck Research Laboratories.

I would indicate to both of you that any written statement you have will be made a part of the record, and you can address us as you see fit, in any way you choose.

As soon as we move this cutting-edge technology stuff out of the way, Dr. Gabriel, you may begin.

STATEMENT OF SHERINE E. GABRIEL, M.D., M.SC., ASSOCIATE PROFESSOR OF MEDICINE AND EPIDEMIOLOGY, MAYO CLINIC, ROCHESTER, MINNESOTA

Dr. GABRIEL. Thank you. Chairman Thomas, Members of——

Chairman THOMAS. I will also indicate to you, Dr. Gabriel, that the microphone is very unidirectional. You will have to pull it down and speak directly into it.

Dr. GABRIEL. Is this better?

Chairman Thomas and Members of the Subcommittee, I am Dr. Sherine Gabriel, a physician and researcher at Mayo Clinic. I thank you for the opportunity to testify before you regarding the important issue of medical records confidentiality.

What I would like to do today is address two fundamental questions bearing on this issue. The first is, What is the importance of medical-records-based research to the public; and the second is, What is the impact of legislation which restricts access to medical records on this category of research?

I am privileged to work at a world-renowned medical institution. The Mayo Clinic's international reputation as a center of excellence in medicine and surgery grew out of the commitment of our founders, Drs. Will and Charlie Mayo, to integrate medical research and education with clinical practice. The Mayo brothers perceived a duty to use information from medical records to evaluate the outcomes of their care and to answer important public health questions and, in 1907, pioneered the concept of the unit medical record, where medical data on each patient is stored in one self-contained packet that is kept in perpetuity.

As you heard earlier from Dr. Borowitz, that is not the case virtually everywhere else in the country, where each provider keeps his or her own personal records about a particular patient.

This concept led to the formation of REP, the Rochester Epidemiology Project. The REP includes a complete medical history of nearly all Olmsted County residents from the time they were born or moved to the county until the time they died or moved away.

The REP is a unique, national research treasury which has been continuously funded by the National Institutes of Health for over 30 years. It has resulted in more than 1,000 scientific publications analyzing dozens of diseases and medical conditions. The central element of the REP is access to the complete medical records of all residents in the geographically defined population.

Medical records research is vital to maintaining and improving the health of the American public. In fact, virtually every health hazard we know of today has been identified using information from medical records. Take AIDS, for example. If researchers had not been allowed to study the medical records of patients with unusual immune deficiency problems in the late seventies, the characterization of the AIDS epidemic would have been delayed at a substantial cost to the public's health.

Similarly, the characterization of Lyme disease required collation of information from the medical records of children who were first presented with this new disease in Lyme, Connecticut.

Other examples include studies examining the benefits and risks of estrogen treatment, as well as the risks of smoking, dietary fats, obesity, and certain occupations.

You may have read than an outbreak of flesh-eating strep was identified at Mayo in 1995. Without access to the medical records of patients with these unusual infections, characterization of this syndrome and isolation of this deadly bacterial strain would have been delayed, and over 100 schoolchildren, which our research showed were the unwitting carriers of this deadly germ in their throats, would have gone untreated.

This discovery lead to the designation of invasive strep as a reportable disease. Such a designation permits recognition and control of epidemics such as the recent outbreak you may have heard about in Texas.

Medical records research is also critical for evaluating the long-term side effects of drugs, the safety of medical devices or procedures, the cost effectiveness of alternative medical practices, and the usefulness of diagnostic tests. Let me give you an example or two in these categories.

Long-term side effects. Nonsteroidal anti-inflammatory drugs, like Advil or Naprosyn, were on the market for decades before medical records research determined these drugs were associated with a higher risk of death due to peptic ulcer disease, particularly in the elderly. This work led to the development of a new class of nonsteroidal anti-inflammatory drugs, soon to be released, which promise a much lower risk of these side effects.

Clinical information for medical records is critical to studies on the safety of medical devices or procedures. For example, studies examining the risk of breast implants.

The cost effectiveness of alternative medical practices could not be established without clinical information from medical records. For example, it was medical-records-based research which determined that a 3-day course of in-hospital bed rest for people with acute low-back pain was just as effective and far less costly as the standard of care at that time of about a 10-day hospital stay.

Finally, it was medical-records-based research at Mayo that led to the discovery of the serious side effects of the diet drug Fen-Phen and its eventual removal from the market.

Every medical advance I have mentioned in the last few minutes relied heavily on information from patients' medical records. Without access to this rich source of clinical information, many of these advances and countless others would not have occurred.

Let me turn quickly to my second question, What is the——

Chairman THOMAS. The light is a guide, Doctor, it is not an absolute necessity.

Dr. GABRIEL. Good. In scientific podiums, there is actually a trap door; and so when the red light goes on, the trap door opens.

Chairman THOMAS. We have one, too. Sit comfortably for a moment.

Dr. GABRIEL. What is the impact of legislation which restricts access to medical records on this category of research?

Legislative restrictions limiting access to medical records threaten the very existence of this entire category of medical research. This is because individuals who refuse to authorize the use of their medical records for research purposes are systematically different in important ways from individuals who do.

The recent Minnesota privacy law provided us with the opportunity to study these differences using a protocol approved by our institutional review board. We found that women were more likely to refuse authorization than men; that persons under 60 were more likely to refuse than older individuals; and persons with certain underlying illnesses, such as mental disorders, breast cancer, or reproductive problems were also more likely to refuse authorization.

That means that studies describing the outcomes of these diseases or the effectiveness or cost effectiveness of treatments excluding these individuals would be biased. They would simply give us the wrong answer. Moreover, studies focusing on these conditions—diseases of women, mental disorders, conditions related to reproduction—would be at even greater risk for incorrect results; and this, in turn, might hamper advances against these important problems.

Finally, while our research was clear on the point that individuals who refuse authorization are systematically different from those who do not, the direction and magnitude of those differences varied from topic to topic. Whereas, you heard the overall average was 4 percent, it varied widely. So not only may such research results result in the wrong answers, but it will be impossible to determine at the outset how wrong they will be or in what direction. Thus, the reliability and validity of findings from such research will be suspect.

Let me illustrate this problem using an example. A study of depression following breast cancer would underestimate the magnitude of the problem if depressed women systematically declined authorization and were thereby excluded. Individuals who experience unsatisfactory outcomes may also be more likely to refuse authorization. If so, a study of a surgical treatment with a high complication rate would underestimate the risks of surgery.

Data such as these form the basis of health care policies, so the examples above could lead to a decision against funding a mental health program to treat depression in women with breast cancer and to a decision to adopt a high risk surgical intervention. Patients need accurate information about health risks, disease prognosis, and outcomes of care in order to make informed decisions.

In closing, I would like to comment briefly on what I believe the reasons are behind the public's strong desire to keep medical information between the patient and his or her physician.

Our research showed that a major concern related to the possibility that insurers or employers might use sensitive information to an individual's disadvantage. This concern is understandable. Although access to medical records for research purposes may be the only access over which the patient is given any choice, there are literally dozens of other opportunities for loss of confidentiality during routine medical care.

For example, in an average outpatient medical encounter in an integrated health care center, such as ours, the following individuals and groups must have access to the complete medical record in order to best serve that patient's needs: the appointment office, the registration desk, the physicians, physician assistants, nurses, EKG, lab, x-ray technicians who perform the necessary tests, and so forth.

In fact, for a typical inpatient encounter, it has been estimated that at least 75 health professionals and hospital personnel have access to the medical record. After all this is taken care of, a qualified nurse researcher, bound by the rules of an IRB and strict patient confidentiality regulations, could be abstracting clinical data from the medical record which will be combined with similar data from hundreds of other patients to answer a specific public health question. The current Minnesota law and other proposed legislation influence only that nurse's access to the medical records and have no impact whatsoever on the 75 other points of access.

Mr. Chairman, such legislation does not ensure the privacy of personal medical information. It does not address the public's concerns regarding potential misuse of personal health information by insurers and employers. Instead, it hinders scientific research and puts the public's health and well-being at risk for serious harm.

Thank you for your attention.

[The prepared statement follows:]

Statement of Sherine E. Gabriel, M.D., M.SC., Associate Professor of Medicine and Epidemiology, Mayo Clinic, Rochester, Minnesota

Chairman Thomas, members of the committee, I am Dr. Sherine Gabriel, a physician and researcher at Mayo Clinic. Thank you for the opportunity to testify before you regarding the important issue of medical records confidentiality.

Today, I would like to discuss two fundamental questions bearing on this issue. The first is: What is the importance of medical records-based research to the public? And the second is: What is the impact of legislation, which restricts access to medical records, on this category of research?

I am privileged to work at a world-renowned medical institution. Mayo Clinic's international reputation as a center of excellence in medicine and surgery grew out of the commitment of our founders, Drs. Will and Charlie Mayo to integrate medical research and education with clinical practice. The Mayo brothers perceived a duty to use information from medical records to evaluate the outcomes of their care and to answer important public health questions and, in 1907, pioneered the concept of the "unit medical record" where medical data on each patient is stored in one self-contained packet that is kept in perpetuity. This concept led to the formation of the Rochester Epidemiology Project (REP) (See Appendix). The REP includes a complete medical history of virtually all Olmsted County residents from the time they where born or moved to the county until the time they died or moved away. The REP is a unique, national research resource, which has been continuously funded by the National Institutes of Health for over 3 decades. It has resulted in over 1000 scientific publications analyzing dozens of diseases and medical conditions, and was ranked in the top 1% of all NIH proposals in 1995. The central element of the REP is access to the complete medical records of all residents of a geographically-defined population.

Medical records research is vital to maintaining and improving the health of the American public. In fact, virtually every health hazard that we know of today has been identified using information from medical records. Take AIDS, for example. If researchers had not been allowed to study the medical records of patients with unusual immune deficiency problems in the late 1970's, the characterization of the AIDS epidemic would have been delayed at a substantial cost to the public's health. Similarly, the characterization of Lyme disease required collation of information from the medical records of the children who first presented with this new disease in Lyme, Connecticut. Other examples include studies examining the benefits and risks of estrogen treatment, as well as the health risks of smoking, dietary fats, obesity, and certain occupations. You may have read that an outbreak of 'flesh eating strep' was identified at Mayo in 1995. Without access to the medical records of patients with these unusual infections, characterization of this syndrome and isolation of this deadly bacterial strain would have been delayed. And over one hundred school children—which our research showed were the unwitting carriers of this deadly germ in their throats—would have gone untreated. This discovery led to the designation of invasive strep as a reportable disease. Such a designation permits earlier recognition and control of epidemics such as the recent outbreak in Texas.

Medical records research is also critical for evaluating the long-term side effects of drugs, the safety of medical devices or procedures, the cost effectiveness of alternative medical practices, and the usefulness of diagnostic tests. Let me give you an example or two in each of these categories. Long-term drug side effects: Non-steroidal anti-inflammatory drugs (those are drugs like Advil or Naprosyn) were on the market for decades before medical records-based research determined that these drugs were associated with higher risk of death due to peptic ulcer disease, especially in the elderly. This work has led to the development of a new class of non-steroidal anti-inflammatory drugs (soon to be released) which promise a much lower risk of these side effects. Clinical information from medical records is critical to studies on the safety of medical devices or procedures, for example, studies examining the risks of breast implants. The cost effectiveness of alternative medical practices could not be established without clinical information from medical records. For example, it was medical records-based research which determined that a 3-day course of in-hospital bedrest for acute low back pain was just as effective and far less costly as the standard of care at that time—a 10-day in-hospital course. Finally, it was medical records-based research at Mayo that led to the discovery of the serious side effects of the diet drug Fen-Phen and its eventual removal from the market.

Every medical advance I have mentioned in the last few minutes has relied heavily on information from patients' medical records. Without access to this rich source of clinical information, many of these advances would not have occurred.

I'd like to turn now to the second question: What is the impact of legislation which restricts access to medical records on this category of research? Legislative restrictions limiting access to medical records threaten the very existence of this entire category of medical research. This is because individuals who refuse to authorize the use of their medical records for research purposes are systematically different in important ways from individuals who do. The recent MN privacy law provided us with the opportunity to study these differences using a protocol approved by our Institutional Review Board (IRB). We found that women were more likely to refuse authorization than men, that persons under 60 were more likely to refuse than older individuals, and that persons with certain underlying illnesses such as mental disorders, breast cancer, and reproductive problems, were also more likely to refuse authorization. Studies describing the outcomes of diseases, or the effectiveness or cost-effectiveness of treatments which exclude such individuals, would be biased—they would give us the wrong answer. Moreover, studies focusing on these conditions, i.e., diseases of women, mental disorders, and conditions related to reproduction would be at greater risk for incorrect results and this, in turn, might hamper advances against these important problems. Finally, while our research was clear on the point that individuals who refuse authorization are systematically different from those who do not refuse, the direction and magnitude of those differences varied from topic to topic and, thus, are completely unpredictable. So not only may such research result in the wrong answers, but it will be impossible to determine how wrong they are, or in what direction. Thus, the reliability and validity of findings from such research will be suspect.

Let me illustrate this problem using a couple of examples. A study of depression following breast cancer would underestimate the magnitude of this problem if depressed women systematically decline authorization and were thereby excluded. Individuals who experience unsatisfactory outcomes may also be more likely to refuse authorization. If so, a study of a surgical treatment with a high complication rate would underestimate the risks of surgery. Data such as these form the basis of health care policies. So, the examples above could lead to a decision against funding a mental health program to treat depression in women with breast cancer and to a decision to adopt a high risk surgical treatment.

Patients need accurate information about health risks, disease prognosis, and outcomes of care in order to make informed decisions about their own medical care. Health care policy makers need high quality data on the costs and outcomes of care provided to all patients (not just a select group) in order to make responsible health care decisions for the population as a whole. The inclusion of all qualifying individuals is the only way to assure that accurate conclusions are drawn about the prognosis of disease, the outcomes of therapy, or the quality of care. Such research can be done while taking appropriate measures for maintaining patient confidentiality, such as careful review and oversight by Institutional Review Boards and strict adherence to procedures restricting access to patient-specific medical information.

In closing, I would like to comment briefly on the reasons behind the public's strong desire to keep personal medical information between the patient and his/her physician. Our research showed that a major concern related to the possibility that insurers or employers might use sensitive medical information to an individual's disadvantage. I understand this concern. Although access to medical records for re-

search purposes may be the only access over which the patient is given any choice, there are dozens of other opportunities for loss of confidentiality during routine clinical care. For example, in an average outpatient medical encounter in an integrated medical center such as ours, the following individuals and groups must have access to a patient's complete medical record in order to best serve that patient's needs: the appointment office, the registration desk, all physicians, physician assistants, and nurses who provide care for the patient, as well as their receptionists and secretaries, all laboratory, medical, nursing and other students and their mentors, EKG, and x-ray technicians who perform the necessary tests, infection control officers who regularly survey medical records for reportable diseases, continuous improvement officers who strive to improve our health care processes and ensure patient satisfaction, the business office for billing, the legal department, and insurers and other third party payers. In fact, for a typical inpatient encounter, it has been estimated that at least 75 health professionals and hospital personnel have access to a patient medical record.1 After all this is taken care of, a qualified nurse researcher, bound by rules of an IRB and strict patient confidentiality regulations, could be abstracting clinical data from the medical record which will be combined with similar data from hundreds of other patients to answer a specific public health question. The current Minnesota law and other proposed legislation influence only that nurse's access to the medical record and have no impact, whatsoever, on any of the other points of access. Mr. Chairman, such legislation does not ensure privacy of personal medical information and does not address the public's concerns regarding potential misuse of personal health information by insurers and employers. Instead, it hinders scientific research and puts the public's health and well-being at risk for serious harm. Your attention should be focused instead on stopping the actual abuses of medical record information that harms patients.

Thank you for your attention.

Chairman THOMAS. Thank you very much, Dr. Gabriel.

Dr. Guess.

STATEMENT OF HARRY A. GUESS, M.D., PH.D., HEAD, EPIDEMIOLOGY DEPARTMENT, MERCK RESEARCH LABORATORIES, BLUE BELL, PENNSYLVANIA; ON BEHALF OF MERCK & CO., INC., WHITEHOUSE STATION, NEW JERSEY

Dr. GUESS. Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to speak with you today on the important issue of protecting the confidentiality of the patient medical record. I am Harry Guess, pediatrician, epidemiologist, and head of the epidemiology department at Merck Research Labs, a division of Merck and Co., a global, research-based pharmaceutical company.

As a physician, I took an oath to protect patients' confidentiality, and we at Merck support the efforts to protect the confidentiality of patient-identifiable medical information. At the same time, care must be taken not to inadvertently harm the interests of patients by unnecessarily restricting the access of medical information for medical research.

As you consider the confidential standards for medical information, I hope you will appreciate how essential medical information and medical records research are to maintaining and improving the health of the American people. To ensure that any legislation or regulations do not jeopardize biomedical research, we believe the following four guides should be followed:

First, legislation should exempt clinical research that is already subject to regulation by FDA, the Food and Drug Administration. This type of research is already stringently regulated by FDA, and

there is strong confidentiality protection for subjects in such research studies.

Second, that legislation would not restrict the use of encrypted or anonymized data. The use of these coded records is critical to medical research and allows, for example, researchers to link encrypted information from several different sources, while ensuring the patients themselves remain unidentified.

Third, the legislation should not discourage collecting and maintaining information necessary to monitor the safety and effectiveness of products that had been approved by the FDA or by foreign regulatory agencies.

Finally, any national standards should preempt conflicting or inconsistent State laws concerning confidentiality. To allow States to add more stringent provisions would risk creating an inconsistent patchwork of requirements that could jeopardize biomedical research. You have already heard about that this morning, very eloquently, from Dr. Gabriel.

Let me give you one example of how regulation of medical information could inadvertently impede the conduct of research that is important to ensuring the safety of medicines.

In 1995 Merck received FDA approval of our chicken pox vaccine. Despite decades of testing in thousands of children, you never really can be sure of what rare yet important safety issues can be found once a medicine or a vaccine is incorporated into broad clinical use. To provide this level of reassurance, we undertook a study in more than 85,000 children to provide further information on the safety of the vaccine under conditions of clinical practice. We conducted the study with pediatricians at the Kaiser Permanente Medical Care Program of Northern California.

The children received the vaccine, with parental consent, as part of their regular medical care. A computer-based search was performed of the medical records of the children receiving the vaccine and of a historical age-matched comparison group of children who had not received the vaccine. The information we received was encrypted so that Merck did not have any patient-identifiable data. The only people with patient-identifiable data were the pediatricians and their staff at Kaiser.

This study provided valuable reassurance about vaccine safety under conditions of broad use in clinical practice and might have been impossible to conduct if it had been required to obtain specific informed consent for the medical records search from all of the parents of the vaccinated children and from the historical comparison group.

This is just one of many examples of medical records research benefiting public health in a way that safeguards the patient-identifiable information.

I thank you once again for the opportunity to express our views on this important topic. We at Merck believe that the confidentiality of patient-identifiable medical information should be protected. We also believe this can be accomplished without jeopardizing either biomedical research or the improvements in health care resulting from the research.

Thank you very much.

[The prepared statement follows:]

Statement of Harry A. Guess, M.D., Ph.D. Head, Epidemiology Department, Merck Research Laboratories, Blue Bell, Pennsylvania; On Behalf of Merck & Co., Inc., Whitehouse Station, New Jersey

I. INTRODUCTION

Mr. Chairman, and distinguished members of the Committee, thank you for the opportunity to speak before you today on the important issue of protecting the confidentiality of patient medical information. I am Dr. Harry Guess, and I lead the Epidemiology department of Merck Research Laboratories, a division of Merck & Co., Inc. Headquartered in Whitehouse Station, New Jersey, Merck is a global, research-driven pharmaceutical company that discovers, develops, manufactures and markets a broad range of human and animal health products—both directly and through its joint ventures—and provides pharmaceutical benefit services through Merck-Medco Managed Care.

The Epidemiology department at Merck is responsible for providing information on diseases to support clinical trials of new drugs or vaccines, and for conducting studies to help evaluate the safety of drugs and vaccines after approval. This work frequently involves collaboration with health care providers to study the safety of drugs and vaccines as they are used in clinical practice. I have also served as an external reviewer of research proposals submitted by managed care organizations to the US Food and Drug Administration (FDA) and the Centers for Disease Control (CDC) to conduct government-funded studies of drug and vaccine safety. I am also an Adjunct Professor of Epidemiology and Biostatistics at the School of Public Health at the University of North Carolina at Chapel Hill, where I teach epidemiology to graduate students.

The purpose of my testimony today is to describe for you how important access to and the use of patient medical information are to medical research. I will (1) describe for you the manner in which we conduct various types of clinical and epidemiological research at Merck and monitor the safety of our marketed products, (2) talk about the types of medical information that we use to conduct that research, and (3) outline some general principles regarding patient confidentiality that we think are key to appropriate legislation in this area.

Let me begin by emphasizing that we at Merck support efforts to protect the confidentiality of patient-identifiable medical information, particularly in light of developments in the area of information technology that have raised questions about levels of individual privacy. All of us are patients ourselves and we certainly recognize the need for protection of privacy. However, from a public health standpoint, we are concerned about simultaneously preserving necessary access to such data for research into new medicines that can cure or prevent disease. In protecting patients' privacy interests, we must be careful not to inadvertently harm the interests of individual patients by unnecessarily restricting access to information needed to determine the safety and effectiveness of medical treatments, assess the usefulness of diagnostic tests, identify disease risk factors, and monitor the cost-effectiveness of new interventions. Such research is needed to continue to be able to provide the American people with health care that meets high standards of safety, effectiveness, and cost-effectiveness. The key to an appropriate legislative solution is to recognize and protect all of those interests.

Innovations in medicine are revolutionizing health care research, as the molecular basis of human disease is revealed. In the past 50 years, medical science has rid the world of smallpox; drastically reduced the incidence of many childhood diseases such as diphtheria, tetanus, polio, measles, whooping cough, and rheumatic fever; and discovered highly effective treatments for many chronic diseases such as asthma, peptic ulcer disease, coronary heart disease, hypertension, diabetes, and osteoporosis. When I trained in Pediatrics nearly twenty years ago, Haemophilus influenzae type b was the most common form of bacterial meningitis among children in the United States, affecting nearly one in every two hundred children. Over the past ten years, the incidence of this devastating disease has been reduced nationwide by more than 95% by the introduction of vaccines.

Given this track record of achievement, the public has come to expect a steady stream of innovations in treatment and prevention from the research-based pharmaceutical and biotechnology industries. In fact, our domestic research-based companies now discover and develop more than half of the new medicines used in the United States and around the world. Merck, for example, has introduced nine important medicines in just the last three years, including CRIXIVAN® for HIV/AIDS, FOSAMAX® for osteoporosis, and SINGULAIR® for asthma in patients as young as six years old, and we are now conducting the research necessary to develop new medicines and vaccines to help patients around the world. Our investment in re-

search will also allow us to enter nine new therapeutic areas by the year 2002, raising our total to 24—the broadest in the industry.

Continued progress of this magnitude clearly depends on broad, multi-faceted research. This includes both basic research in chemistry, molecular biology, genetics, and pharmacology, which allows us to understand disease processes and identify the right compounds to combat the disease, and clinical research to evaluate the safety and efficacy of potential new medicines and vaccines. Finally, large-scale epidemiologic and health services research studies are needed to help us design new clinical trials and to monitor how well treatments work in clinical practice. For example, epidemiologic research helped show us that while aspirin can reduce the risk of heart attacks in adults, it can cause a serious life-threatening illness called Reye's syndrome when administered to children with chickenpox or influenza. Reye's syndrome has been almost completely eliminated as a result of this discovery.

With that general background in mind, we would like to propose the following four principles, to help guide legislation on confidentiality of medical information. I will first outline the principles, then discuss the types and use of patient information used in medical research and safety monitoring, and finally discuss each of the principles in more detail.

(1) Clinical research that is subject to regulation by the Food and Drug Administration should be exempted from any new confidentiality requirements because this research is already subject to strict confidentiality protections;

(2) Only information that directly identifies an individual should be subject to confidentiality requirements; use of anonymized, encrypted or encoded data should be excluded from restrictions on access;

(3) Legislation should not inhibit the collection and maintenance of information to monitor or verify the safety and efficacy of approved products; and

(4) There must be uniform national standards that preempt conflicting or inconsistent state laws.

II. Background—Different Types of Patient Medical Information

Before I describe the various ways or settings in which pharmaceutical researchers use patient medical information, I think it would be useful to explain the three different types of patient information that we use. First, and most pertinent to our discussion of confidentiality, is information that directly identifies individuals, by providing a name or address, for example. For purposes of our discussion today, I'll refer to this type of information as "patient-identifiable" information.

The second type of information is referred to as "encoded" or "encrypted" information. In my testimony today, I will use the term "encrypted." This type of information is patient-identifiable information from which personal identifiers and means of directly contacting the individual (such as name, address, and social security number) have been replaced with a code, which is often in the form of a long number. The identity of such an individual is not apparent from the information itself or from the code, but may be determined by use of the encryption key. Encryption keys have two important functions. One is to permit the keyholder to identify the patient in the event that this becomes necessary—for example if a safety problem is discovered that requires notifying the patient. The second function is to be able to "link" one data set with another data set on the same patients without having to reveal patient identities. For example, a study may provide information on a group of patients who receive medical evaluations at yearly intervals. By linking together all of the visits on each patient, one may evaluate changes in medical conditions over time without having to reveal any patient-identifying information. One may also link encrypted information from pharmacy files to encrypted information from hospitalization records in such a way as to study the safety and effectiveness of drugs in very large populations without revealing any patient-identifying information. Essentially all patient information used in the research that I do is in an encrypted format, and the linking mechanisms allow for information about an individual contained in two or more data sets to be combined without revealing the identity of any individuals.

The third type of information I will refer to as "anonymized," which means information from which all personal identifiers have been removed, and/or information that has been aggregated in such a manner that the identities of individuals who are the subjects of the information cannot be identified under any circumstances. There would be no means to identify individuals, dis-aggregate or link this information to other data sets containing information about such individuals by use of a code or a key. Information that is anonymized in this fashion is generally much less useful for research than is encrypted data because it may lack the detail that is required for meaningful or sophisticated analyses. Also, with anonymized data it

would never be possible for anyone to notify the subjects if a safety problem were discovered or if it became highly important to obtain additional information. Nevertheless, we do use such anonymized information in certain specific areas of research, which I will discuss in more detail below.

It is important to keep the differences between these types of patient information in mind, because concerns about privacy are different with information that is encrypted or anonymized than they are with patient-identifiable information.

III. Use of Medical Information—In Clinical Trials

Now I would like to describe for you some of the ways in which pharmaceutical researchers use these different types of information, and how patients' confidentiality interests are protected. I would like to begin with a brief overview of the clinical drug development process, and the roles that FDA and Institutional Review Boards (IRBs) play in that process.

Before testing any new drug in humans, a sponsor such as Merck must run a potential new drug candidate through comprehensive animal pharmacology and toxicology studies. With those and other pertinent data in hand, the sponsor files an Investigational New Drug application, or IND, with the FDA. The agency has a fixed period of time to evaluate the IND application and notify the sponsor if the agency judges the application not to be sufficient to justify undertaking human clinical trials. Upon completion of the FDA review of the IND, the sponsor begins the clinical study program.

The clinical program is designed to demonstrate the investigational drug's safety and efficacy in treating, preventing or diagnosing a disease or condition in humans. It is the most time-consuming and resource-intensive segment of the drug development process, including third party clinical investigators, institutional review boards (IRB's), FDA regulation and involvement, and, in many cases, thousands of study subjects, or individual patients. Today the process is made even more complex because companies such as Merck generally seek approval of new drugs not only in the United States but in many foreign countries. Consequently, such trials are subject not only to FDA regulations but also to regulations by many foreign regulatory agencies. Safety reports must be filed with these agencies and different agencies may require differing types of studies to evaluate efficacy.

While the design of clinical trials will vary from drug to drug and from disease state to disease state, there are some general similarities in their typical overall structure, or "phases" of development. This phased approach allows researchers to build upon information and knowledge generated during the preceding phases as they broaden their study of the drug.

"Phase 1" studies are designed primarily to assess the clinical safety of the drug in humans, and to determine whether the compound is sufficiently safe to be studied further in humans. These studies usually involve a limited number (approximately 20 to 80) normal healthy adults, who can be kept under close medical observation and monitoring for a short period of time.

If the data generated during the Phase 1 studies are acceptable, the sponsor can begin "Phase 2" studies, which are intended to demonstrate (1) the drug's efficacy in treating the disease or condition in humans, and (2) common or short-term adverse effects and risks that might be associated with the use of the drug. Phase 2 studies may also help establish the most appropriate dose of a drug. Such studies may involve up to several hundred patients, who are treated under conditions of close medical observation and monitoring.

In "Phase 3" trials, the number of patients participating expands significantly (involving several hundred to several thousand subjects) in order to study the drug's use in conditions that more closely resemble those that would exist after approval. The study group should be adequately representative in order to allow the generalization of the results to the population at large. Depending on the disease or condition being studied, study subjects can generally be treated on an outpatient basis, and medical monitoring is usually less strict than during the earlier phases. Phase 3 studies intended to provide the evidence of efficacy necessary for drug approval must typically meet four criteria: they should be (1) controlled (one group receives the investigational drug and another group receives either a placebo or an active drug known to be efficacious), (2) double-blind (neither study subjects nor investigators know which patient is receiving which therapy), (3) randomized (study subjects randomly assigned to treatment groups), and (4) of sufficient size to provide a statistically sound test of efficacy.

All of these clinical studies are subject to extensive FDA regulations, including protection of patient confidentiality and the requirement that an IRB approve the studies before they can be initiated. The IRB's primary function is to minimize risks

to the subjects, and to assure that the subjects are adequately informed about the trial and their treatment. The regulations require that the IRB be sufficiently qualified through the experience and expertise of its members to promote and to safeguard the rights and welfare of study participants. The IRB has five members, each appointed by the institution involved, such as the hospital or academic institution at which the study is being conducted. Race, gender, cultural backgrounds, and sensitivity to community issues may be considered in appointing members. The IRB must include individuals with the necessary expertise and professional competence to review proposed research for compatibility with institutional commitments and regulations, applicable law, and standards of professional conduct and practice, and should include both women and men as members. Its members may not consist entirely of members of one profession. At least one member must have scientific expertise, usually a physician, and at least one member must have a primary interest in non-scientific areas. One member must not be affiliated with the institution or have an immediate family member who is affiliated with the institution; that person is often a member of the clergy or other representative of the broader community.

The IRB reviews the study protocol, and is authorized to require changes to the protocol if necessary. The IRB weighs the potential risks to the patients versus the potential benefits. To approve a research study, the IRB must determine that the study meets seven criteria specified in FDA regulations, including, "where appropriate, [that] there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data."

FDA regulations also require that no humans may be subjects in FDA-regulated research unless the investigator has obtained the "legally effective informed consent of the subject or the subject's legally authorized representative." To obtain a subject's "informed consent," the regulations specify that information regarding eight basic elements must be provided to the subject, and six additional elements should be discussed "when appropriate." One of the mandatory elements is a statement that describes the extent to which confidentiality of patient records will be maintained, and notes the possibility that the Food and Drug Administration may inspect the records, including patient-identifiable information. The regulations also require that the subject's informed consent be documented, using an IRB-approved written consent form signed by the subject or his or her legal representative. The IRB reviews the patient informed consent forms, and may require revisions to strengthen or clarify them if needed.

The clinical investigator—the physician who is actually working with the study subjects—keeps patient-identifiable information for all of the study subjects, just as any treating physician would. This is critical to the investigator's ability to provide follow-up care to these patients, and to be able to contact them, if necessary, if some safety issue should arise. The study sponsor, such as Merck, receives only encrypted data from the investigator.

Thus, in a clinical trial program, the study subjects have expressly consented to the researchers' use of their medical information. The IRB assures that there are adequate provisions in place to protect patients' confidentiality and the privacy of their data. We do not believe that there is any need to require any further protections in this area.

You may hear some mention of the "Common Rule" in discussions about confidentiality in research projects, and I want to explain the connection between the Common Rule and the FDA regulations I talked about before. The Common Rule refers to the common standards for the protection of human subjects involved in research conducted, funded or regulated by 16 federal agencies, including the Department of Health and Human Services (DHHS). Those standards were published as a final rule in the Federal Register on June 18, 1991. The FDA had previously adopted regulations on the protection of human subjects in research that it regulates, published at 21 CFR Parts 50 and 56. Those regulations were largely consistent with the principles embodied in the Common Rule. On June 18, 1991, the FDA published a final rule that modified its existing regulations to conform them with the Common Rule to the extent possible. There are some minor variations due to FDA's unique statutory mission under the federal Food, Drug & Cosmetic Act. However, because the DHHS has adopted the Common Rule as applicable to all research with human subjects that it regulates, funds or conducts, clinical research that is subject to FDA regulation is also subject to the Common Rule to the extent that the two are not inconsistent. Where the Common Rule and the FDA regulations differ, the FDA regulations would govern.

IV. Use of Medical Information in Epidemiological and Outcomes Research

Generally, epidemiologists study populations to understand the extent, natural course and burden of disease. This information provides background for the safe and effective use of medicines. In contrast to clinical trials (which are experimental), an epidemiologic observational study tracks patients in the real world of clinical medicine. It is this science that is used to evaluate the risks and benefits of medications in large numbers of patients in a "real world setting." Epidemiologic studies have had a major impact on the public's health in general, and on our understanding of the risks and benefits of medications, in particular. For example, these studies documented the relationship between aspirin and Reye's Syndrome in children, and the risk of vaginal cancer in daughters of women who took diethylstilbestrol (DES) while pregnant. They have also been instrumental in documenting risks and benefits of vaccines, oral contraceptives, and a number of other widely used medications. Clearly, epidemiologic studies are critical to the future of public health.

One of Merck's sources of data includes information in the public domain. This type of data is encrypted by the agency or organization supplying the data, and can be obtained from regional, national and international claims-based and survey data. Examples include survey data from the National Center for Health Statistics, or Medicare data from the Health Care Finance Administration. Public-use data is provided in an anonymous or encrypted form in which the user is not able to identify individuals who participated in the survey or study. This information may be used to determine the prevalence of a disease, or incidence of a disease relative to that found among users of an approved drug. We are not alone in our use of these important databases—the CDC, the National Institutes of Health (NIH) and other government institutions utilize these registries to track public health statistics, identify disease trends, and assess the economic impact of new medical and surgical treatments.

Although large public-use databases are extremely valuable, they do not provide all of the necessary information needed to make drugs available to patients. Therefore, additional studies which involve either direct contact with a patient or collection of encrypted medical information are necessary. These studies collect information on what kinds of patients are likely to develop the disease, how well existing treatments work, what the types and rates of complications are, what costs and medical care utilization are associated with the disease, and what the long-term consequences of the disease are. Such information is needed to design clinical trials necessary for drug or vaccine approval. We generally conduct such studies in collaboration with managed care organizations, universities, or federal agencies such as the NIH or CDC. We use the data from these sources in encrypted or anonymized aggregate form. Within this context, we cannot—nor would we have the desire or need to—identify an individual patient who has participated in these types of studies.

The information collected in this manner provides background for new clinical trials and also supports drugs that have been approved for use. This type of research is different from a clinical trial because it involves analysis of data under conditions of ordinary clinical practice, which can be different from the conditions in a clinical trial. The additional risk to the patient in being involved in this type of data review is minimal, since we are studying the treatment and care provided by the patients' own physicians and the impact of that treatment on the disease or condition. In contrast to a clinical trial, researchers are not proposing any particular treatment, prescribing any medications or providing any medical care. Medical information regarding a medical condition or the patient's health status is obtained via medical record review under the direction of the treating clinic or facility, or by third party patient interviews. In either case, Merck receives only data that is encrypted or in anonymized aggregate form.

In support of clinical trials, these data are used to:

- Determine how many patients should be included in a clinical trial in order to minimize patient risk while maximizing clinical trial results
- Provide background on the incidence or prevalence of a disease
- Provide information on current treatment practices
- Aidin determining the appropriate patient population to include in the trial
- Provide data on the usefulness of questionnaires to assess safety and quality of life

In addition to supporting clinical trials, outcomes and epidemiology research is also used to

- Identify risk factors for developing a disease
- Determine the long-term outcome of a treatment on disease

- Identify patient populations who may not be receiving state of the art treatment or therapy
- Identify prognostic factors and risks of disease complications
- Determine the impact of a treatment on quality of life
- Assess utilization of resources and provide information on the economic benefits of a treatment

The importance of using encrypted patient-level data may be demonstrated by several studies that have impacted the health of the public and aided in the development of important drugs. For example, in collaboration with the government of Saskatchewan, we used encrypted data on all of the one million residents of that Canadian province to evaluate the risk of rare adverse events associated with use of drugs to treat arthritis in very elderly patients. For the past nine years we have been collaborating with investigators from Mayo Clinic as well as from Japan and Europe to study the long-term course of prostate diseases in men. This study has contributed numerous publications to the medical literature and greatly increased medical knowledge.

We are currently conducting an epidemiology study in conjunction with a university to determine the prevalence of low bone mineral density, a measure of osteoporosis, in nursing home residents. This study will also determine what factors predict hip fracture in these patients. Patients must undergo a bone scan and allow the researcher access to their medical records, but the information gained from studying the records of these patients may provide insight into ways we can enhance the quality of life of nursing home residents by preventing hip fractures. The university IRB has approved the study, and all subjects have provided informed consent. The university researchers conducting the study provide us only with encrypted or anonymized data.

In another study, we used clinical trial data combined with data published in the literature to articulate the economic value of a treatment with CRIXIVAN®, our protease inhibitor for the treatment of HIV/AIDS. The clinical trial data was from our original clinical trials conducted before FDA approval of the product, and all study subjects had given informed consent to the use of their medical information. We simply re-examined those data in conjunction with the additional published data to simulate the long-term progression of the disease. The purpose of the cost-effectiveness model is to assist healthcare providers, payors and other decision-makers in determining health, reimbursement, and clinical policies. This model suggests that initiation of therapy with CRIXIVAN® alone and in combination with AZT and 3TC before the first AIDS-defining illness increases survival at a cost that is generally accepted by current standards.

V. Post-Approval Safety and Efficacy Monitoring and Reporting

In its role as the federal agency charged with helping to ensure the public health and safety relating to the use of drug products, the FDA has established extensive regulations to monitor the safety of drugs, biologics, and medical devices. FDA regulations impose on pharmaceutical companies mandatory reporting requirements for adverse experiences associated with the use of drug products in humans. To meet their obligations under this regulatory scheme, manufacturers must have access to patient medical information. These regulations contain stringent reporting time deadlines and record-keeping requirements that apply to both investigational drugs and marketed products. The purpose of the adverse experience reporting regulations and procedures is to support the FDA's efforts to protect the public safety by providing the agency with information necessary to determine the safety profile of investigational and marketed drug products.

The vitality of this safety reporting system is critical to identifying safety issues in use of marketed products that were not identified in investigational studies. The reporting system is used to evaluate the seriousness of potential health problems and to alert the agency and health care community to take appropriate corrective actions.

Because of its limited resources, the FDA heavily relies on manufacturers to investigate reports of adverse experiences with their drug products. Manufacturers most often receive such reports directly from the treating physician for the patient involved. Sometimes patients themselves report their own adverse events. Whenever a manufacturer receives notice of an adverse experience associated with any of its products, the manufacturer is required to investigate the incident and to provide the information to the FDA. If additional information is not obtainable, a follow-up report is required to explain what steps were taken to obtain additional information relating to the adverse experience and why the information could not be obtained. The more detailed information that can be obtained about a particular adverse expe-

rience, the better informed the manufacturer, the FDA and the health care community can be about the safety profile of marketed products. By necessity, this requires knowledge about confidential medical record information. In fact, FDA's 1997 Guidance on adverse experience reporting specifies that before submitting any adverse experience reports to the FDA, a manufacturer must have four specific pieces of information, including "an identifiable patient." This does not mean that the reporting physician must supply the manufacturer with the patient's name; the reporting physician can provide the manufacturer with encrypted information on a specific patient, as long as follow-up information can be obtained from the physician if necessary.

The FDA has issued regulations to ensure that the identities of patients and those who report adverse experiences are held in strict confidence and are not disclosed by the FDA or by manufacturers who possess these reports. Manufacturers are required to encode patient identifying information before submitting reports to the FDA, but must maintain sufficient information to permit additional information to be obtained, if necessary, from the person who reported the event. Moreover, the identity of the adverse experience reporter, usually the patient's health care provider, must be deleted when reporting to the FDA. These privacy protections were instituted to enable the FDA to continue to collect information on safety risks associated with FDA-regulated products that is considered vital to protection of public health. In addition to the need to comply with FDA reporting requirements, Merck must also comply with the reporting requirements of foreign regulatory agencies. Typically an agency from a given country will want to be made aware of worldwide safety information on all products which are approved in that country. Because of this, Merck will often have to supply foreign regulatory agencies with information on adverse events occurring in patients in the United States. Foreign regulatory agencies also respect the need for patient confidentiality and hence do not require any patient-identifiable information.

Learning more about the safety profile of marketed products may not be limited to reports that meet the regulatory definition of adverse drug experiences but may also include additional information that may lead to a better understanding of certain aspects of a product's safety profile. Thus, for example, many drug and vaccine products are contraindicated for use in pregnant women because of a lack of clinical study information about the safety of the product for use in that patient population. Yet, manufacturers may choose voluntarily to collect and report to the FDA information about a drug product's use during pregnancy even though that use is not associated with an adverse experience. Information on use during pregnancy may be collected from health care professionals who report such use to drug manufacturers or the FDA. At Merck, we treat such information in the same manner as we treat information associated with adverse experience reports. The purpose of collecting and reporting this information is to enhance our knowledge about the overall safety profile of a product in pregnant women.

VI. Principles for Legislation

As you consider confidentiality standards for medical information, I hope you will appreciate how vital medical information and records research is to maintaining and improving the health of the American public. Research on new medicines vitally depends upon patients' participation in clinical trials and researchers' access to their relevant medical information as well as to patient-level archival databases.

In order to ensure that any new legislation, regulation or standards do not jeopardize biomedical research, we believe that the following four guides should be followed.

First, clinical research subject to regulation by the Food and Drug Administration should be exempt from any new or additional requirements. This is because, as explained above, this type of research and use of information is already stringently regulated by the FDA through application of the Common Rule, which, in turn, provides strong confidentiality protection to the subjects of clinical trial research.

Second, access to and use of anonymized or encrypted data should be excluded from any new requirements or restrictions applicable to information that identifies patients. Only data sources or collections of samples that directly identify individuals should be subject to confidentiality protections, since information that does not identify an individual cannot violate one's confidentiality interest. In addition, the code numbers should be permitted to be used for the purpose of linking to additional information about subjects in a database without triggering unnecessary or burdensome requirements, so long as the subjects remain unidentified.

Third, legislation should acknowledge and encourage the collection and maintenance of information to verify or monitor the safety and efficacy of products that have been approved by the FDA or international regulatory authorities.

And finally, uniform national standards that preempt conflicting or inconsistent State laws concerning confidentiality are necessary. Individual states should not be able to add to or detract from federal rules in this area that is so critical to improving the public health through research yielding better medicines. To allow states to add more stringent provisions would risk creating an inconsistent patchwork of requirements that will at best confuse and at worst seriously jeopardize biomedical research projects. Researchers whose primary concern should be quality and integrity of study design and execution should not also be faced with the additional complexities of satisfying inconsistent state requirements for research that crosses state lines.

VII. CONCLUSION

I thank you once again for the opportunity to express our views on this important topic. We at Merck believe that the confidentiality interests of patients in their medical information can and should be protected. We also believe that this can be accomplished in a way that does not jeopardize biomedical research and the quality and improvements in healthcare that result from that research.

Chairman THOMAS. Dr. Gabriel, I guess for most of us, if you say health in Minnesota, you think of the Mayo Clinic. My concern was, how did Minnesota wind up passing a law which probably wounded significantly one of its cash cows from a pure mercenary point of view? Did you work with the legislature prior to the passage of the law? Was there a relatively high level of understanding among the legislators of the consequences of their decision?

Dr. GABRIEL. I cannot speak directly to that because I was not involved, but I know that some of my colleagues were involved, and the extent to which there was a complete understanding of the consequences, I guess I cannot speak to that.

Chairman THOMAS. Has there been a followup with the Minnesota legislature after the passage of the law so that they could understand the consequences?

Dr. GABRIEL. Yes, the law has recently been amended. When the law was first put into place, as you may know, it required us to put in place a very complicated and costly computerized system, which you alluded to earlier.

Chairman THOMAS. And you chose to do it because you thought it was important.

Dr. GABRIEL. We chose to be in full compliance. And that is no longer required. That level of compliance is no longer required, according to the amendment.

Chairman THOMAS. And according to your testimony, and this is one of my concerns, again operating, if in fact we do, on an anecdotal basis or an incomplete understanding of what we are doing, Minnesota apparently created the system that plugged one leak that may or may not have been a leak of the information source by dealing with the nurses but left open myriad areas of leakage, which, in fact, if an investigation were carried out, were probably the primary sources of leaks, if leaks occurred. Is that a relatively accurate statement?

Dr. GABRIEL. That is my impression. Any legislation that focuses strictly on research access would do exactly the same thing. I listed

in my written testimony not all 75 but certainly all of the other points of access where leakage could occur.

I think the main concern is that legislation should address the concerns of the patients. And from our research, which we did on our local population, the main concern of the patient is not that a nurse abstracter will collect information and remove identifiers and lead to a published study. The main concerns are the issues of discrimination, that were brought up before, and the misuse of information by employers and insurers.

Chairman THOMAS. Dr. Guess, I can understand the narrow focus of your testimony in terms of Merck carrying out research and wanting us to stay away from FDA and the rest, but your example of Kaiser providing you with a research component, that was real-world and actually off of ordinarily collected data, which indicates to me that what we maybe need to focus on is not "what" but "who and why." If we can get the "who and why" right, then the "what" is less of a concern, except when you go to the patient-identifiable data level, which is of great concern.

I am talking more about your area of research and the encrypting. I am not so wild about building barriers between FDA and HHS in terms of collecting data. I know you are, and you have to go it based upon who you are here for, but I am more interested in getting it right on all of the data that may flow than creating pockets of accuracy or I like what I have, so leave me alone. Any reaction?

Dr. GUESS. Well, sir, I really agree with the tone and the overall scope of your testimony. I think the concern we have about FDA is that we are subject to such stringent regulation in so many ways with FDA that adding another layer of complexity on top of that could create problems.

Chairman THOMAS. I would be concerned about layering, but if they are doing something right there, I want to borrow it and apply it in other areas, if it makes sense. I know it is a relatively narrow area you are dealing with, but in areas where there has been complete ability to maintain confidentiality, I want to look at those.

Dr. GUESS. Right. I think the issue with FDA is that, with drug research under FDA regulations, it is all interventional. So one can obtain informed consent from the subjects in a clinical trial, but in a retrospective data base search, where you are looking through anonymized records of several thousand people, some of whom may have moved away, because it is historical data, there would really be a problem of applying that paradigm in a sort of slavish way.

Chairman THOMAS. Thank you.

Does the gentleman from California wish to inquire?

Mr. BECERRA. If I could continue that line of questioning. Are there then some aspects of the FDA protocol which would be most useful as we are trying to come up with ways to protect privacy in every other aspect of research and disclosure that occurs?

Dr. GUESS. Well, I think, as I said in my testimony earlier, that for encrypted or anonymized data, we feel that to subject that to the kinds of provisions we have with FDA studies could create a real burden. I think when it comes to patient-identifiable data, which is really the concern, I think some of the provisions we have with FDA do make sense.

When we collect primary data on identifiable patients or when investigators collect that, it does make sense to have stringent provisions on that. But when we obtain anonymized data, where we do not know who the patients are, I think that is a very different situation.

Mr. BECERRA. For either of the two panelists, what is the whole issue of the fact that more and more we are finding that medical research and answers to medical dilemmas are really more than just national in scope, they are really global? The whole AIDS epidemic is certainly one of those illnesses or diseases that falls within that category.

How do you go about establishing privacy laws that will be sufficient if the European Union on one end has very stringent privacy laws and we may have other countries in other parts of the globe who probably do not have any at all, and if they do, they may not be enforced? How do you go about doing the research going beyond the U.S. border and ensuring that as you try to collect information which will give you the best result for your research that you are also providing the privacy that people deserve?

Dr. GUESS. I would be happy to take that, since we do research on a global scale.

I do not claim to be an authority on what is going on in the European scene, but I do know the pharmaceutical industry is working with the European Union to try to create a code of conduct that will enable pharmaceutical research, specifically clinical research, to be carried out in a way that is not impeded by some of the privacy initiatives in Europe.

I feel the problem is actually more a problem with some of the proposed initiatives in Europe actually inhibiting research in a way that becomes inappropriate and actually harmful to them.

I will say in certain countries in Europe, such as Germany, for one, and France, to a certain extent, for another, epidemiologic research and health services research is very underdeveloped relative to what it is in the United States. As you go down the list of things that Dr. Gabriel mentioned, virtually all of those discoveries are American-based discoveries. We have a very strong force in that area.

Dr. GABRIEL. Could I respond to that?

Mr. BECERRA. Yes, of course.

Dr. GABRIEL. I think what you said also speaks to the importance of preemption, so that at least in the United States, we can have a common approach and a unified approach to these problems.

As far as the international scene, there are a number of international epidemiology and research groups that are now assembled. I am part of a couple of them that are devising international standards for these studies and trying to discuss that with the regulatory agencies in their own settings.

Mr. BECERRA. Thank you, Dr. Gabriel.

If I can follow up on that, where would you break on the issue of preemption in view of what you just said?

Dr. GABRIEL. Well, Mayo Foundation operates in five different States. That means the clinical practice as well as the clinical research crosses State boundaries, and it makes very little sense for us to have this patchwork of rules and regulations. It really ham-

pers both the practice and the research activities. So we would be in favor of it. However, I do agree with one of the previous speakers about the value of having States do their own reportable disease and public health work. I think that is a different category. But, in terms of confidentiality, I think it makes a lot of sense for integrated health care delivery systems such as ours that operate in more than one State to have one set of rules.

Mr. BECERRA. Dr. Guess, if I could return to the whole issue of what you face in Europe as you try to conduct research, is part of the difficulty that you have in Europe or in certain European countries, is it due more to commercial issues or factors here than it might be actually conducting the research where, for example, they may want to keep their particular research market closed to their researchers that are home based?

Dr. GUESS. I do not actually think so. I think some of the privacy initiatives there may come about because much of the health care is socialized, and so I think it is a privacy tradition. Also, the German privacy tradition has its origins in other problems, and so I do not think it is really a commercial interest. I think it just stems from the way the health care is organized.

Mr. BECERRA. You mentioned that that has caused Merck and other U.S. pharmaceuticals problems in trying to conduct the research necessary.

Dr. GUESS. Well, I think if certain of the provisions were to go through, problems would be caused.

I will also say that much of the type of research we do, for example the study that we did at Kaiser, could not have been done in many parts of Europe. So there are certain things that, just from their very cumbersome restrictions, would be quite difficult to do in many parts of Europe. I do not mean to take Europe as a whole, but in many parts of Europe would be quite difficult to do.

Mr. BECERRA. Thank you.

Mr. Chairman, if I could ask one last question.

How does the European Union treat the various nations within the Union? Are they provided with particular discretion? For example, a European Union-wide preemption. Does that exist?

Dr. GUESS. I think the objective with the European Union directive is to create some uniformity to the European requirements, and they are working toward this right now. So they are trying to create some sort of preemption of a patchwork of national laws right now. But the problem may be setting the level at an appropriate level.

Mr. BECERRA. Thank you. Thank you, Mr. Chairman.

Chairman THOMAS. I would tell the gentleman this is going to be an ongoing area in which, if we do not coordinate between the European Union, the more emerging union of the European Union, than we have in the past, where the historical situation of drug companies going to Europe to do certain types of testing and research because of the laws in the United States making it more difficult—that if, in fact, the European Union moves on the basis in large part of anecdotal or other reasons for restricting that research, we have the opportunity, were we to get it right, to carry on the research here.

But if we do not change other areas of the law, we will not have the ability to do it, notwithstanding the fact that we have now created an opportunity to transmit the information in a confidential way. So that what we do here is not the complete story. We have to deal with the opportunity to allow research to go on beyond the patient records and the collection of data.

It would be an ultimate irony if the European drug companies, if there are any left after those laws are passed in Europe, would be coming to the United States to do the kind of research where the populations make sense on an analogous basis. Where they do not, Merck and other companies, obviously, are moving around the globe; and what I would very much like to do is get it right and set a model which is appropriate so that we can at least urge others to follow our example.

I want to thank all of you for the testimony that was given, and especially the last panel. Without any additional questions, the Subcommittee stands adjourned.

[Whereupon, at 12:10 p.m., the hearing was adjourned.]

[Submissions for the record follow:]

American Association of Health Plans

I. INTRODUCTION

The American Association of Health Plans (AAHP) is the largest national organization of health plans. AAHP represents more than 1,000 health maintenance organizations (HMOs), preferred provider organizations (PPOs), and similar network-based plans. Together, AAHP member plans provide quality health services for approximately 140 million Americans. AAHP member plans are dedicated to a philosophy of care that puts patients first by providing coordinated, comprehensive health care.

The subject of today's hearing—how to craft federal legislation to protect against inappropriate use of patient-identifiable health information, while at the same time permitting the coordination and delivery of high quality health care—is one of the most important issues facing federal health policy makers today. Not only is there great potential for harm if patient information is misused, but our health care system relies on patient trust as an essential ingredient to quality health care. The use of patient information by health care providers, health plans, and health researchers has already greatly improved the quality of health care. Continued use of this information will enable us to build on that improvement.

Chairman Thomas, members of the Committee, and staff have been extremely open to discussing this issue with AAHP and our member plans, and we appreciate their efforts to develop workable, real-world policies and procedures regarding the confidentiality of patient-identifiable health information.

This statement highlights how health plans currently use patient-identifiable health information to support quality assurance and improvement programs and emphasizes the importance of properly structuring federal confidentiality legislation in order both to preserve patient confidentiality and ensure that quality of patient care can continue to be enhanced.

II. HEALTH PLANS SUPPORT SAFEGUARDING THE CONFIDENTIALITY OF PATIENT-IDENTIFIABLE HEALTH INFORMATION

AAHP and its member plans strongly support the goal of assuring consumers that health plans and health care providers will respect the confidentiality of their identifiable health information. We believe that appropriate confidentiality safeguards for patient-identifiable information are essential to ensuring that health plan members feel comfortable communicating honestly and openly with their physicians and other providers. Without open communication between patients and their providers, treatment decisions are based on incomplete or inaccurate information and quality of patient care suffers.

AAHP's member plans have demonstrated their commitment to confidentiality by addressing this issue as part of AAHP's ongoing Putting Patients First initiative. Because AAHP is committed to addressing the issue of consumer confidence in health plans, association members must meet standards related to confidentiality. Member plans must safeguard the confidentiality of patient-identifiable health information through policies and procedures that, consistent with federal and state law, (a) address safeguards to protect the confidentiality of patient-identifiable health information; (b) provide for appropriate training of plan staff with access to patient-identifiable information; and (c) identify mechanisms, including a clear disciplinary policy, to address the improper use of patient-identifiable health information. The policy reinforces that health plans should not disclose patient-identifiable health information without the patient's consent, except when necessary to provide care, perform essential plan functions such as quality assurance, conduct bona fide research, comply with law or court order, or for public health purposes.

This policy on confidentiality joins other policies that are also part of AAHP's Putting Patients First initiative, covering areas such as information for consumers, physician-patient communication, choice of physician, grievance and appeals, physicians' role in plan practices, and, of course, quality assessment and improvement.

Virtually all of the current federal legislative proposals related to confidentiality recognize that health plans need access to patient-identifiable information for purposes of facilitating treatment and securing payment for health services. However, one area where there continues to be some confusion over health plans' need for information relates to health plans' efforts to improve quality of care.

It is true that, for some of the quality-enhancing activities health plans undertake, they are able to use non-identifiable health information—information that has been aggregated, anonymized, coded, or encrypted in such a way that the information no longer reveals the identity of particular individuals. Consistent with the vast majority of legislative confidentiality proposals that have been considered to date, AAHP believes that a patient's interest in confidentiality is pertinent only when his or her identifiable information is involved. Because aggregate, anonymized, coded, or encrypted information does not identify individuals, consumers need not be concerned about the use of this information.

However, some of the fundamental, quality-enhancing activities undertaken by health plans do require the use of identifiable health information. The use of health information in health plan quality assurance and improvement activities can greatly enhance the quality of health care for both the individual plan member and the member population as a whole, and AAHP believes that health plan members should benefit from these quality improvement activities. These activities are not only fundamental to coordinated, quality care, but in many cases are also required of health plans under a variety of state and federal programs and regulations, as well as under voluntary private sector reporting and accreditation standards.

III. Health Plans Use Patient-Identifiable Health Information to Enhance Quality

Health plans use patient-identifiable health information in a variety of activities that improve the quality of health care. These activities, which focus on both the processes of delivering care as well as on the outcomes of care, include health promotion and prevention, disease management, outcomes research, and utilization management. Health plans' ability to enhance quality through these activities could be seriously jeopardized unless federal confidentiality legislation is properly structured.

Health Promotion and Prevention

Health promotion and prevention activities improve quality by enabling plans and providers to identify members at risk for certain illnesses or eligible for certain services. Plans and providers can then reach out to those members to provide information to them and encourage them to seek out services when they can benefit most from intervention and before disease progresses. Often, determining who is at risk involves the use of patient-identifiable health information. Health plans add much of value in this area because they have access to claims data and can help busy physicians accurately identify patients at risk of certain illnesses or who are eligible for certain services—even among patients the physician may not have seen in some time. Once the plans have identified these members, they contact them and, in many cases, the members' physicians as well. Many plans encourage their physicians to follow-up with the identified members to schedule the necessary appointments.

For example, nearly all plans have implemented postcard or phone-call mammography reminder systems for their female members. Patient-identifiable information is used to identify female enrollees of a certain age who have not received a recent mammogram. United HealthCare's plans use patient-identifiable information to single out women aged 50 to 74 who are overdue for a mammogram. The plans send reminder notices to these women as well as to their physicians so that the physicians can follow-up with their patients directly. As a result of this program, in 1995, United HealthCare's plans across the country experienced increases in mammography rates ranging from 30–45%. This program and others like it promote detection of breast cancer in the earliest and most treatable stages.

Disease Management

Disease management activities improve quality by identifying members who have been diagnosed with certain chronic diseases and then coordinating and monitoring their care. Again, because health plans have access to claims data, they are well-positioned to identify those members who will benefit most from disease management programs. Health plans then contact the identified members and, in many cases the members' physicians, in order to encourage them to seek the appropriate care.

For example, according to a recent study, 45.4% of all HMOs had diabetes disease management initiatives in place in January 1996.[1] Harvard Pilgrim New England has developed a comprehensive gestational diabetes management program that includes directed case management and regular vision screenings. The plan uses patient-identifiable information to identify members with diabetes and involve them in the plan's disease management program. As a result, the plan was able to increase annual retinal exams by 26%, eliminate diabetes-related newborn major malformations, and decrease the incidence of low blood sugar reactions in patients receiving insulin therapy.

Asthma management is another area where health plans use patient-identifiable information to target members and improve the quality of care delivered to them. As of January 1996, 50.4% of all HMOs had asthma management programs in place.[2] PrimeCare Health Plan, for example, examines clinic and hospital record information to identify children with asthma who are missing an inordinate number of clinic appointments and who have high hospital admission rates. Working with the children's pediatricians, the plan involves the children and their families in an asthma education and management program that initially resulted in a 30% reduction in emergency room visits and a 60% reduction in hospital admissions for participants of the program.

Outcomes Research

Another method health plans use to improve the quality of care is outcomes research. Health plans use patient information to evaluate the effect of particular treatment programs, assess the typical course of a chronic disease over time, and identify variations in outcomes that may be targeted for future improvements in health care processes.

For example, Kaiser Permanente of Northern California used patient-identifiable information to study the most effective treatment for a type of diabetes. Using identifiable health information of their members who had been treated for diabetes, Kaiser studied whether patients who matched a certain clinical profile and were treated with the drug Metformin experienced better outcomes than patients who did not have the same profile but who were also treated with Metformin. The outcomes analysis indicated that, in fact, outcomes were better in the patients who matched the profile than in those who did not match the profile. This study provided Kaiser physicians with the clinical evidence needed to select the most effective course of therapy for their diabetic patients.

Utilization Management

Utilization management activities involve evaluating the medical necessity and appropriateness of health care services both for the purposes of payment as well as for quality improvement. Utilization management enables plans to respond to inappropriate patterns of care. For example, evidence suggests that hysterectomies and caesarean section deliveries are over-performed in the U.S. Hysterectomies are the second most common procedure—performed on 1 in 3 American women by the age of 60. In Italy, by comparison, the figure is 1 in 6 and in France it is only 1 in 18. Similarly, the Centers for Disease Control estimated that physicians performed

[1] The InnerStudy Competitive Edge Part II: Industry Report, September 1996, p. 76.
[2] Ibid.

349,000 unnecessary caesarean section deliveries (approximately 1 out of every 12 deliveries) in 1991—unnecessarily placing women at risk of infection and unnecessarily exposing them to the complications and trauma associated with major abdominal surgery. Health plans' utilization management programs require patient-identifiable information to ensure that patients receive necessary, appropriate, high-quality care in a cost-effective manner.

Integrated Delivery of Services

Integrated delivery of services enables health plans and providers to utilize patient-identifiable health information in even more ways to improve the quality of care. Often, physicians are provided with increased access to patient information in order to aid them in their management of certain health conditions. For example, physicians at LDS Hospital in Salt Lake City created a computer-assisted management program for antibiotics and other anti-infective agents which Intermountain Health Care now uses in its hospital intensive care settings. The program compares historical patient data (rendered non-patient-identifiable) on infection characteristics and antibiotics effectively used in treatment to current patient infection data. The system then provides decision support to physicians by recommending anti-infective regimens and courses of therapy based on its comparison. The system also helps to prevent adverse drug reactions and promote cost-effective care by enabling physicians to choose anti-infective regimens that are the most effective for the lowest cost.[3] In this example, patient-identifiable information that has been rendered non-identifiable is used to link previous patient record information on infection causes and treatment regimens to the computer-assisted antibiotic management program to improve care for current patients.

As previously mentioned, not only are these activities that use patient-identifiable information fundamental to improving patient care, but many are also required of health plans under a variety of state and federal programs and regulations, as well as under voluntary private-sector reporting and accreditation standards. For example:

- Activities to monitor, detect, and respond to over- and under-utilization are required by state HMO and utilization review laws, federal laws, and private accreditation standards;
- Data collection and analysis of condition-specific patient outcomes are required of plans participating in the Federal Employees Health Benefits Program;
- Ongoing quality assurance programs that (1) stress health outcomes and provide for the collection, analysis, and reporting of data; (2) monitor and evaluate high volume and high risk services and the care of acute and chronic conditions; and (3) after identifying areas for improvement, take action to improve quality, are required of Medicare+Choice plans under Medicare;
- Procedures to ensure health care delivery under reasonable quality standards, consistent with recognized medical practice standards, and ongoing, focused activities to evaluate health care services, are required by the NAIC Model HMO Act, which approximately 30 states have adopted;
- Quality management programs that "monitor, evaluate, and work to improve the quality of care and quality of services provided . . . utilizing a variety of quality management studies, reviews, and evaluations such as . . . medical record reviews" are required of plans seeking URAC/AAHCC accreditation;
- Quality management standards that monitor aspects of patient care such as disease management, acute and chronic care, and preventive care are also required of plans seeking URAC/AAHCC accreditation;
- Health management systems that identify members with chronic conditions and offer appropriate services and programs to assist in managing their conditions are required of plans seeking NCQA accreditation; and
- Actions and interventions to improve quality by addressing opportunities for improved performance are also required of plans seeking NCQA accreditation.

It is clear that health plans' efforts to improve patient care have been recognized by state, federal, and private regulatory entities alike. It also should be clear that compromising plans' abilities to improve patient care—whether by imposing excessive regulatory requirements or by leaving plans with inadequate or partial information for quality studies—would result in reduced quality of care. This would present an obvious quandary for plans legally and contractually required to conduct quality-enhancement activities, yet at the same time forbidden to use the information necessary to fulfill these obligations.

---

[3] Evans RS, Pestotnik SL, Classen DC, et. al., "A computer-assisted management program for antibiotics and other anti-infective agents," New England Journal of Medicine, January 22, 1998; 338:232–8.

IV. Unduly Restricting Health Plan Use of Patient-Identifiable Health Information Would Reduce Quality

Some of the current federal confidentiality proposals include provisions which would unduly restrict health plan use of patient-identifiable health information and, as a result, seriously threaten quality of care. One of the more restrictive and quality-compromising approaches put forth would be to require health plans and providers to obtain patient authorization each and every time they use identifiable health information. This type of authorization requirement would be impractical, costly, and a major burden for patients as well as for plans. Moreover, the nature of many of these plan activities is that they are seeking to identify individuals at risk—it would be impossible to obtain consent from individuals who had not yet been identified. As a result, health plans would be unable to send mammography reminder notices or information on asthma management programs to plan members in need of these services.

A second approach to restricting the use of patient-identifiable information for quality-enhancing purposes which has also been proposed by some would be to permit patients to opt-out of participating in quality-enhancing activities, such as health promotion, disease management, outcomes research, and utilization management. Such an opt-out provision would diminish the capacity of current health plan quality assurance programs and be counterproductive to improving the quality of patient care. In fact, withholding some patients' information within a health plan setting could make engaging in these quality-enhancing activities so impractical that plans and providers would forgo these activities for all patients—again, raising the potential conflict between plan obligations to improve quality and legal restrictions on the use of the information needed to fulfill those obligations. For example, in the case of the computer-assisted management program for antibiotics, if patients were permitted to object to the use of their medical record information for this program, the data available to physicians would be incomplete and could skew the computer-generated treatment recommendations, potentially threatening the quality of care not just for the patient who opts out, but for all current patients. Such a threat could likely prompt the discontinuation of this innovative and much-lauded program. This would also be true for other quality-enhancement endeavors of this type.

Leaving plans with incomplete information could also force current state, federal, and private reporting and quality improvement requirements to be modified and weakened to reflect the health plans' diminished capacity even to report on health outcomes or enrollees' use of services. This in and of itself would make plan quality improvement less effective and accreditation status less meaningful. On a more global level, our national goal of finding out the most effective ways to deliver health care—to make sure that patients get the best care for their health dollar—would be severely compromised.

V. A Statutory Authorization Would Preserve Quality of Care With Fewer Procedural Barriers

For the reasons just mentioned in the previous section, AAHP supports the inclusion of a statutory authorization in federal confidentiality legislation. A statutory authorization would authorize in law all of the widely accepted positive uses of patient-identifiable health information, including facilitating treatment, securing payment, and conducting health plan quality-enhancing activities. Both the Administration's proposal and the National Association of Insurance Commissioners' (NAIC) draft Health Information Privacy Model Act follow the statutory authorization approach. A statutory authorization would achieve the goal of providing plans and providers with access to identifiable health information to improve quality of care. And, by working in tandem with strong penalties for the misuse of identifiable health information, a statutory authorization would also achieve the goal of assuring consumers that plans and providers will respect the confidentiality of their identifiable health information. It is AAHP's recommendation that any penalties be consistent with the penalties already established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for the wrongful disclosure of individually identifiable health information.

A slightly less effective alternative to the statutory authorization that has also been proposed is the consolidated authorization. As proposed, the consolidated authorization would allow plans to procure a single authorization at the time of enrollment to use identifiable health information for the purposes of facilitating treatment, securing payment, and conducting quality improvement activities central to patient care. While the consolidated authorization is a vast improvement over having to obtain separate authorizations each and every time patient-identifiable infor-

mation is used, this approach has limitations that the statutory authorization does not.

For example, one legislative proposal that has followed the consolidated authorization approach has also included provisions permitting revocation of that consolidated authorization. Yet, expecting health plans to facilitate and pay for quality health care services after a patient has revoked his or her prior authorization for use of health information is a Catch-22 for health plans. Not being able to use patient-identifiable information would interfere with plans' abilities to effectuate payment for services already rendered, facilitate and coordinate treatment, and fulfill legally required operational functions—in essence, paralyzing plans' ability to effectively serve patients. On the other hand, plans—and physicians and hospitals—could be held criminally liable for continuing to facilitate high quality treatment by using identifiable information.

This particular legislative proposal has addressed this dilemma by giving health plans explicit permission to disenroll individuals from the plan upon the individual's revocation of his or her authorization. While health plans prefer not to have to disenroll patients, revocation provisions often provide them no choice. In fact, given the liability involved for unauthorized use of information as well as for substandard care, revocation by an enrolled individual should perhaps be treated as disenrollment without requiring any further action by the plan. It should also be noted that plans may have underway at the time of an individual's revocation quality improvement activities, such as outcomes research, that would continue to require the use of the patient's identifiable health information lest the entire endeavor be compromised by an individual's withdrawal of his or her information mid-study. This again points to the superiority of the statutory authorization approach.

VI. The Same Level of Protection Should Be Required for All Types of Patient-Identifiable Health Information

AAHP believes that federal confidentiality legislation should require the same level of protection for all types of patient-identifiable health information. Health care providers rely on the completeness of medical records in their treatment of patients. Segregating certain types of health information, such as genetic information, from the rest of the medical record could interfere with a provider's access to health information that can just as easily be a predictor of future health problems as other types of health information. Because of this, current practice in most health plans supports uniform treatment of all health information and, in many cases, genetic information is an integral part of the medical record indistinguishable from other personal health information. For example, given a notation of a positive marker for one of the breast cancer genes in a patient's record, a physician can encourage increased mammography screenings to detect any breast cancer tumors at an earlier and more treatable stage.

Moreover, oftentimes genetic information may not be any more sensitive than other medical record information. HIV status, treatment for mental health, reproductive history, or evidence of sexually transmitted disease can be considered equally sensitive information. Because many types of health information can be considered sensitive, singling out information based on its presumed sensitivity would only promote inconsistent protections.

With advanced software capabilities available, it is far preferable to limit access to information through the use of passwords and other software controls than to require plans and providers to physically store different types of information separately or treat different types of information differently.

VII. There Should Be Nationally Consistent Rules in Areas that Affect Computerized Information Systems

AAHP believes that, given the complex and interstate nature of the way information flows in today's health care system, federal confidentiality legislation should address the need for nationally consistent rules in areas that affect computerized information systems. Moreover, consistent rules governing disclosure of various portions of computerized health records will facilitate compliance by multi-state health plans and employers.

VIII. Patients Should Have the Opportunity to Inspect, Copy, and Request Amendment To Their Identifiable Health Information

AAHP supports patients having the opportunity to inspect, copy, and request amendment to their identifiable health information. Federal confidentiality legislation should recognize, however, that health plans that arrange for services through

provider networks typically do not maintain central medical records files. While health plans that employ salaried physicians and those that contract with physician groups whose practice is solely focused on serving the health plan's members may be prepared to provide their members with access to a comprehensive medical record, even members of these plans may occasionally seek care outside of the plan's affiliated providers. Given that it is a provider who originates health information, we believe it is appropriate for providers to be responsible for facilitating access to records and appropriate amendment procedures. Federal legislation should permit health plans to direct patients wishing to inspect, copy, or request an amendment to their record, to their physician or other provider who originated the information in question.

In addition, some proposed legislation includes a requirement to include patients' written requests for amendments and written statements of disagreement in the patient's medical record. However, for the growing numbers of plans and providers that utilize electronic medical records, this requirement would entail transforming the patient's written statements into electronic format in order for it to become part of the medical record. Instead, AAHP suggests that a notation concerning the patient's request to amend or statement of disagreement fulfill any such requirement.

IX. Research

Any provisions targeted to research in federal confidentiality legislation must ensure that intra-plan quality improvement and other health plan operational activities are not suddenly subject to a federal oversight process that was intended for the protection of human subjects participating in clinical research and that was never intended to encompass routine quality improvement activities related to health care treatment and payment. Intra-plan quality improvement activities should not be subject to federal oversight.

Federal confidentiality legislation must also ensure that those health plans and providers that wish to provide patients access to clinical trials may continue to do so without being subject to a federal research approval process. Current federal oversight of clinical trials already subjects researchers to review by an independent board specially designed to protect and safeguard the interests of human subjects.

X. Conclusion

AAHP wholeheartedly supports the goal of assuring consumers that health plans and health care providers will respect the confidentiality of their identifiable health information. At the same time, AAHP believes that consumers should benefit from the quality-enhancing activities health plans undertake—many of which are required by public regulators and private sector oversight entities. In order to craft federal confidentiality legislation that achieves these two goals, it is essential to have a firm understanding of how our current health care system works, how information flows within the system to make it work, and how health plans use information to improve the quality of health care.

In this statement, AAHP has highlighted the following recommendations for federal confidentiality legislation:

(1) Federal confidentiality legislation should not unduly restrict health plan use of patient-identifiable health information. Instead, legislation should statutorily authorize the use of patient-identifiable health information for the purposes of facilitating treatment, securing payment, and conducting health plan quality improvement activities central to patient care. This statutory authorization would work in tandem with penalties for misuse that are consistent with HIPAA.

(2) Federal confidentiality legislation should require the same level of protection for all types of patient-identifiable health information.

(3) Federal confidentiality legislation should address the need for nationally consistent rules in areas that affect computerized information systems.

(4) Federal confidentiality legislation should permit health plans to direct patients wishing to inspect, copy, or request an amendment to their record, to their provider. In addition, any requirements to include written statements submitted by the patient in the patient's record should permit plans and providers to include a notation of that a written statement exists if it is more technologically feasible to do so.

(5) Any research provisions included in federal confidentiality legislation must be carefully constructed to ensure that intra-plan quality improvement activities are not suddenly subject to a process that was intended for the protection of human subjects participating in clinical research and that was never intended to encompass routine quality improvement activities related to health care treatment and payment. In addition, any research provisions must ensure that those health plans and providers that wish to provide patients access to clinical trials may continue to do

so without being subject to a federal research approval process. Current federal oversight of clinical trials already subjects researchers to review by an independent board specially designed to protect and safeguard the interests of human subjects.

We look forward to working with the Committee in its continued work on federal confidentiality legislation.

Statement of American Association of Occupational Health Nurses (AAOHN)

The American Association of Occupational Health Nurses, Inc. (AAOHN) appreciates the opportunity to submit written testimony to the House Committee on Ways & Means, Subcommittee on Health for the hearing record on the matter of Health Care Information Privacy and Confidentiality. We want to thank the Chairman and express our special appreciation for his leadership on this important issue.

Our primary interest in participating in these hearings is to urge Congress, in the strongest terms, to enact truly comprehensive medical records confidentiality legislation. In summary, we believe that for Congress to be successful in this area, it must craft legislation that will ensure that all medical records are protected under the law regardless of the mode of payment or the setting where the health information is obtained or maintained.

AAOHN is the professional association for more than 13,000 occupational and environmental health nurses who provide on-the-job health care for the nation's workers. Occupational health nurses are the largest group of health care providers at the worksite. As such, our professional nurses assume responsibility for all aspects of health and safety for individual workers and the work environment. AAOHN supports the development of uniform laws, rules and procedures governing the use and disclosure of health care information. AAOHN has had a long-standing interest in the debate on confidentiality of health information. The Association has developed position statements and guidelines on the issue to ensure that the voice of the occupational and environmental health nurse is heard in Washington.

BACKGROUND

In the course of their jobs, occupational health professionals collect personal information about the health and lifestyles of their company's employees. AAOHN members are responsible for a great deal of data collection and maintenance of personal health information. This often includes records that document medical and/or health surveillance activities, wellness programs, pre-job placement and return-to-work physical examinations, and other similar types of worksite health initiatives. It is our observation that, to date, the confidentiality issues surrounding the protection of health information gathered and maintained at the worksite have gone largely unnoticed in the confidentiality debate. Health care information obtained and maintained at the worksite is both personal and sensitive. Clearly, health information records found at the worksite are as important to the confidentiality interests of the nation's workers as the patient data contained in the more traditionally thought of medical record. Worksite information, if improperly used or released, may be equally as harmful to an employee's interests as unauthorized disclosure of more traditional medical records.

AAOHN maintains that employers should have access only to that amount of health information necessary to determine whether a worker may perform his or her job in a safe manner. For example, we believe that in cases of fitness for work exams (e.g., health surveillance, pre-job placement and physical examinations, and return-to-work physical examination records) health care professionals should provide the employer with a written determination based on the medical record rather than handing the employer the actual record itself.

Also, in cases in which workers' compensation benefits are at issue, information obtained through the company's wellness or employee assistance programs should not be used to defeat the claim. Employees seeking medical or disability payments under state workers' compensation laws should not be forced to sign releases covering their entire medical record in order to file their claim. Only information directly relevant to the illness or injury underlying the compensation claim and any appropriate secondary injury determination should be available. No other information should be released without meaningful, uncoerced consent on the employee's part for a more expansive disclosure.

Limiting the amount of personal health information an employer may learn about his or her employee is not a novel or untested regulatory approach. The "bloodborne

pathogens" regulations issued by the Occupational Safety and Health Administration (OSHA) explicitly requires that such information must be kept confidential and "not disclosed or reported without the employee's express written consent to any person within or outside the workplace except when required by this section or as may be required by law." [1]

The law also narrows the extent of the information provided to the employer to that which is necessary to make a determination regarding work fitness. For example, the regulation states that the "healthcare professional's written opinion .... shall be limited to whether (a particular treatment) is indicated for an employee, and if the employee has received such (treatment)." [2]

We believe that Congress should enact a law to protect individually identifiable health information utilizing the standards set forth in the bloodborne pathogens regulations.

To be clear, occupational health professionals have an ethical obligation to safeguard health information confidentiality. AAOHN's ethical tenets caution against inappropriately disclosing confidential information yet recognize, however, that there are a number of appropriate ethical and legal exceptions to the rule. For example, it is perfectly ethical and legal to disclose information concerning threats of homicide, threats of suicide, reportable diseases, child or elder abuse, any injury caused by firearms or other violent acts, and other information covered by law. Other types of disclosures for specific purposes such as controlled research, emergencies, civil, judicial and administrative purposes, law enforcement, oversight and payment may also be appropriate.

Employers must be able to access certain personal health information when considering pre-placement testing, fitness for work exams and work place safety health testing. Specific limited information must be available to employers making reasonable job accommodations in cases of disability or reviewing claims for workers' compensation benefits. In addition, because employers are also responsible for providing a number of other types of benefits such as health and disability insurance, family medical leave and employee assistance programs, they may require that certain specific health information be disclosed. AAOHN firmly believes that employers should be allowed to administer these important programs in an efficient manner.

Unfortunately, occupational health nurses are often pressured by employers to release a workers' entire medical record. As such, the occupational health professional is caught between management demands and the nurse's ethical responsibility to protect the employee's confidentiality. Many of our members can attest to the fact that employers often pressure occupational health nurses to divulge the confidential health information of their employees. For too many occupational health nurses this ethical and legal dilemma is not a theoretical issue. The cases of Bettye Jane Gass and Kathleen Easterson provide two such examples:

Bettye Jane Gass

Bettye Jane Gass became a registered nurse when she passed her Kentucky Nursing Boards in 1975. She received her degree in nursing from Western Kentucky University. Shortly thereafter, Ms. Gass began working at both Western Kentucky University and the Lord Corporation on a part-time basis. She later left the employment of Western Kentucky University to become a full-time Health Services Specialist at the Lord Corporation's Bowling Green plant.

In that position Bettye Jane Gass was responsible for providing treatment to employees who sustained injury or became ill. She was also responsible for maintaining the case histories of workers; coordinating paper work flow for injury compensation reports; scheduling pre-employment physicals and follow-up physician visits; preparing summaries and reports; and maintaining OSHA record-keeping requirements as well as coordinating activities of the company's wellness program. She was asked to return to part-time status in 1993 and was terminated on September 7, 1995, without prior notice after approximately thirteen and one-half years at the Lord Corporation.

On that date, the human resource manager demanded access to the routine physical examinations given to all plant employees. Betty Jane Gass refused to turn over the keys to the filing cabinet where the worksite health information was kept. She refused to violate her ethical obligations and despite a written company policy that expressly stated that health services personnel should maintain confidentiality and provide limited access to the medical files, she was fired for "insubordination." The state court that heard her case issued a summary judgment stating that Ms. Gass "failed to show that her discharge was in violation of any fundamental and well de-

[1] 29 CFR Ch. 1910.1030.
[2] Id.

fined public policy as evidenced by a constitutional or statutory provision." Bettye Jane Gass has filed an appeal and the case is still in pending litigation.

Kathleen Easterson

In the case of Kathleen Easterson, the issues of employer pressure resulting in the termination of an occupational health nurse are again presented. Kathleen Easterson, an occupational health nurse and Assistant Director of Nursing and Director of Employee Health at a New York area medical center, was terminated by her employer when she refused to disclose the contents of a doctor's note containing an employee's non-occupational diagnosis of severe headache and TMJ trauma. Like the case of Bettye Jane Gass, the termination occurred despite the fact that there was an explicit corporate policy pertaining to medical records confidentiality.

In the court case that followed the hospital's actions, Ms. Easterson sued for wrongful discharge and reinstatement of employment. Ms. Easterson explained to the court that she believed that the worker in her care had a reasonable expectation of privacy with respect to the medical records kept in her care. She believed this to be true because of the existence of the nurse-client confidential relationship. She explained to the court that the employer's policy and practice of reviewing an employee's medical record without consent should not be tolerated. If employers were allowed to continue this policy, she argued, it would erode trust in the health care system and should therefore, be held to be against the interests of good public policy. Ms. Easterson maintained that the doctor's note was part of the employee's confidential record and that there was no governmental compulsion to reveal the employee's medical record.

Unfortunately, the two lower courts that heard the case held that there was no nurse-client relationship between the occupational health nurse and the employee. In addition, the court held that the doctor's note at issue was not information acquired by the nurse in attending the employee/client. The court also found that the doctor's note was not necessary to enable the nurse to act in a nurse-client capacity. The court determined that the doctor's note did not create a substantial and specific danger to the public health. Finally, the court determined that there was no basis in law upon which to provide Ms. Easterson with relief for her claims.

AAOHN believes that the lack of legal recourse in both the Gass and Easterson cases is egregious and should be corrected through Congressional enactment of comprehensive confidentiality legislation.

GREATER PROTECTIONS SHOULD BE CREATED UNDER FEDERAL LAW

AAOHN maintains that workers must be allowed to feel that their private disclosures will be treated in a dignified and confidential manner. The existence of the patch work of state laws does not always provide such assurances in the worksite setting. Under the laws of many states, employers are not prohibited from accessing detailed personally identifiable employee health information with the company. This is true because the occupational health professional is viewed as an agent of the employer, not as a health care provider with a duty of confidentiality to the patient-employee. In addition, courts have found that physicians representing employers are not bound by the physician-patient duty of confidentiality.[3]

At the same time, health care professionals have been held liable in some states for violations of their professional duty to respect privacy. For example, when a private physician notified an employer that an employee had a "long-standing nervous condition with feelings of anxiety, and insecurity," the patient won an award for damages from the physician because the patient had asked not to have the information released and because the court could find no compelling reason for the disclosure.[4]

In another case, the West Virginia Supreme Court held that under the state's workers' compensation statute, physicians can allow employers access to written medical reports but not to information collected from oral communications. The court also ruled that employees can sue both their physicians for releasing confidential information and their employer for requesting the information.[5]

In still other cases, health care professionals have *not* been held liable in at least one state that has attempted to protect patients from unfair information practices, for arguably the wrong reasons. In a Maryland case, a plaintiff named Leo Kelly, Jr., brought suit against a physician named Dr. Brad Lerner based on medical malpractice. In that case the parties agreed to submit the claim to binding arbitration.

---

[3] *Rogers v. Horvath*, 237 N.W. 2d 595 (Mich. 1995).
[4] *Horne v. Patton*, 287 So.2d 824 (Ala. 1974).
[5] *Morris v. Consolidation Coal*, 446 S.E.2d 648 (W.Va. 1994).

The plaintiff hired an expert witness named Dr. Horst Schirmer to testify that Dr. Lerner had breached the standard of care by performing an operation known as a transurethral resection of the prostate ("TURP") on the plaintiff.

On cross-examination, Lerner's counsel sought to impeach Schirmer by introducing a copy of a pathology report that indicated that Dr. Schirmer had performed the identical surgery under conditions he alleged constituted a breach of care on the part of Dr. Learner. The subject of that pathology report was William Warner. Based on this use of his medical records, Warner sued Learner alleging that a violation of the Maryland Confidentiality Records Act of 1990, resulted from Lerner's improper taking and use of Warner's medical records without his prior consent. *Warner v. Lerner*, 115 Md. App. 428, 693 A.2d 394 (1997). Lerner filed a motion to dismiss the case which the Court granted on the grounds that the law stated that in litigation "a health care provider may disclose a medical record without the authorization of a person in interest." Despite the fact that the Maryland legislature intended to protect patients from violations of their confidentiality, they did not foresee that health care providers such as Dr. Lerner would use a provision apparently intended to allow physicians to defend themselves in malpractice actions for other purposes. The Court stated:

[w]e are troubled here ... [d]espite this Court's quite obvious discomfort, maybe even displeasure, or its severe reservations regarding just what was intended by the general assembly, the language of the statute is clear, and we must give meaning to those words as those words set forth by that deliberative body.

This case points out some of the more egregious perils and pitfalls that exist in the current patch work quilt of state confidentiality laws.

AAOHN believes that workers must be provided with adequate confidentiality safeguards regardless of where the personally identifiable health information is obtained or maintained. We believe that Congress, therefore, must enact comprehensive uniform medical record confidentiality legislation in order to protect both workers and occupational health professionals. Without an appropriate amount of carefully crafted legal protections, health care professionals will continue to have difficulty in protecting workers' personal health care information and struggle with the burdens of carrying out their ethical obligations.

THE "MEDICAL INFORMATION PROTECTION ACT OF 1998" (DRAFT)

AAOHN has indicated its support for a number of elements contained in the latest draft version of the "Medical Information Protection Act of 1998," prepared by Senator Robert Bennett (R–UT) and co-sponsored by Senator Jim Jeffords (R–VT). Although this bill has not been introduced in either the Senate or House we commend several sections of this proposal to your attention. In general, we believe that this proposal would provide sufficient protections without creating unreasonable burdens on participants and providers in the health care system. The proposal prescribes the following federal standards that would:

- provide individuals with access to their own health information and the right to make corrections;
- impose civil and criminal penalties for wrongful disclosure and mishandling of protected medical records;
- limit an individual's personally identifiable health information that could be disclosed without consent to certain specified circumstances (e.g., emergencies, health research conducted by an approved certified institutional review board, fraud and abuse, etc.); and
- require that a notice of confidentiality practices be posted in public.

In general the proposed legislation would also preempt state law.

AAOHN supports defining the "term health information" broadly enough to include medical records obtained or maintained at the worksite for purposes other than treatment or payment. We also support the draft bill because it would require that entities that create health information post a notice of their confidentiality practices. The simple practice of posting such a notice, we believe, will allow employees an opportunity to gain a clearer understanding of their rights. It will also provide employees with a better understanding that individuals do, indeed, have the power under the law to take legal action against violators when appropriate.

In addition, we are encouraged by the bill's criminal sanctions provisions because we believe it is essential that those who would knowingly and intentionally obtain personally identifiable health information and disclose this information in violation of the proposed law be penalized.[6]

[6] The "Medical Information Protection Act of 1998," Title III, Subtitle A, Section 301(a).

We suggest, however, that the draft bill could be strengthened by extending penalties to those circumstances in which individuals are "attempting" to obtain personally identifiable information for purposes of unauthorized disclosure. It is not enough, in our view, to merely penalize those who are successful at inappropriately obtaining and disclosing personally identifiable health information. The recent news stories regarding the highly aggressive marketing practices of certain health related corporations remind us that greater protections are essential. The change we propose would improve the bill and serve as a significant deterrent against inappropriate disclosures. We note that at least one previous draft version of the bill contained this important provision and suggest that any further drafts would be greatly improved by including the old provision in the final bill prior to its introduction.[7]

We also support providing uniform legal protections across the nation. Without a broad uniformity provision, conflicts will arise due to the fact that it will not always be obvious that a specific state law does provide for "greater protections" than the federal law. While we believe enacting a weaker preemption provision would be an improvement over the status quo, we suspect that anything less than full preemption could lead to more litigation and confusion rather than less.

Finally, AAOHN is actively working to ensure that any legislation that moves through Congress includes a provision that would clarify that the law should not require a health care provider within an entity (e.g., a physician or nurse who provides occupational health services) to disclose protected health information to others within the company or entity. This issue is often complicated and steeped in terminology that courts may find unfamiliar. Under the Bennett-Jeffords approach, it appears clear that health information concerning wellness records and first aid would be protected but that other types of worksite records may not be covered. We urge you and others to include in any confidentiality legislation a provision that would protect employee medical records related to fitness to work as well as those records that document the treatment of illness or injuries or participation in wellness or employee assistance programs. While we prefer that this important concept be included in actual legislative language, we want to also offer the following suggested Report language:

The Committee believes that the health provider who creates, originates or maintains the health information within the entity is the proper person to determine whether a disclosure is consistent with the limitations under subsection (d). The intent is to protect the confidentiality of an individual's medical records in the workplace, especially those related to an employee's fitness to work (e.g., medical surveillance records, health screening, return-to-work physical examination records).

In summary, we believe this type of language would limit the releases of important information to protect employee confidentiality while allowing employers to operate their worksite health programs appropriately.

THE CLINTON ADMINISTRATION'S RECOMMENDATIONS

As you know, in September of 1997, Secretary of Health and Human Services Donna Shalala provided your Committee with a number of recommendations regarding standards for privacy and protection of individually identifiable health information. These recommendations were in fulfillment of her duties required by the Health Insurance Portability and Accountability Act (HIPAA). While not legislation, these recommendations put forth the following five important principles:

- Boundaries: An individual's health care information should be used for health purposes and only for those purposes, subject to a few carefully defined exceptions. It should be easy to use information for those defined purposes, and very difficult to use it for other purposes. Federal health record confidentiality legislation should impose a legal duty of confidentiality on those who provide and pay for health care, and on other entities that receive health information from them;
- Security: Organizations to which we entrust health information ought to protect it against deliberate or inadvertent misuse or disclosure. Federal law should require such security measures;
- Consumer Control: Patients should be able to see what is in their records, get a copy, correct errors, and find out who else has seen them. [The Administration's] recommendations significantly strengthen the ability of consumers to understand and control what happens to their health care information;
- Accountability: Those who misuse personal health information should be punished, and those who are harmed by its misuse should have legal recourse. Federal

[7] See, "Medical Information Confidentiality Act," Title I, Subtitle B, Section 311(a)(1). Version, (0:/BAI/BAI97.721). Fall 1997.

law should provide new sanctions and new avenues for redress for consumers whose privacy rights have been violated; and

- Public Responsibility: Individuals' claims to privacy must be balanced by their public responsibility to contribute to the common good, through use of their information for important, socially useful purposes, with the understanding that their information will be used with respect and care and will be legally protected. Federal law should identify those limited arenas in which our public responsibilities warrant authorization of access to our medical information, and should sharply limit the uses and disclosure of information in those contexts.

AAOHN is convinced that personal health information can be collected and effectively utilized in the workplace without sacrificing the employee's right to privacy if employers conscientiously follow Secretary Shalala's principles. Unfortunately, the Secretary envisions defining employer "activities that use health information" too narrowly to fully protect the privacy interests of American workers. Addressing only the privacy issues raised by employers' access to traditional treatment, payment, wellness and first aid records still leaves employees significantly at risk because of the potential for employers' misuse of information in other types of worksite records. AAOHN and its members know from experience that business can operate effectively while adhering to well-thought-out policies that guarantee the confidentiality of personally identifiable health information. Such policies provide adequate physical, administrative and technical safeguards against nonconsensual intra-company disclosures of employee data that exceed the scope of information legitimately needed by the employer to run its business safely and effectively.

AAOHN urges Congress to expand upon Secretary Shalala's recommendations and to enact a medical records confidentiality statute that adequately protects all employee health information held at the worksite not just those records mentioned by the Secretary.

CONCLUSION

Mr. Chairman, AAOHN greatly appreciates this opportunity to offer our comments for the hearing record. In addition to our specific comments, we offer the following five principles that we believe will be useful as Congress deliberates on this important issue:

- First, define health information broadly enough to include all medical records obtained or maintained at the worksite for purposes other than treatment or payment;
- Second, require entities that create or maintain health information to post a notice of their confidentiality practices;
- Third, apply the guiding principles of compatibility of purpose and minimal disclosure to all personally identifiable health information available to an employer regardless of the reason why the employer holds or has access to the records;
- Fourth, recognize that the health care professional who creates, originates or maintains the health information at a worksite is the appropriate person, rather than management, to determine whether a disclosure is consistent with the purposes underlying the reason for the release of the information;
- Lastly, include penalties for coercing or attempting to coerce inappropriate record disclosures as well as penalties for actual misuse.

These elements are essential components of any comprehensive federal medical records confidentiality law intended to protect the personal health information of America's workforce. We urge Congress to keep principles in mind when legislating, and we look forward to working with you and your colleagues as this important matter moves through the legislative process.

Statement of American College of Occupational and Environmental Medicine, Arlington Heights, Illinois

The American College of Occupational and Environmental Medicine (ACOEM) is pleased to have the opportunity to submit testimony to the House Committee on Ways and Means, Subcommittee on Health on the issue of confidentiality of medical records and Secretary Shalala's recommendations for legislation.

ACOEM, representing over 7,000 physicians, is the world's largest medical society committed to promoting and protecting the health, safety, productivity and well-being of people at work and in their environment.

ACOEM supports the development of uniform comprehensive legislation addressing the confidentiality of medical records. The College feels that such legislation should include provisions that encompass the treatment of employee medical information in the workplace.

There is great potential for a worker to be adversely affected by the misuse of workplace medical records. Decisions on return to work, job placement, and promotion can be influenced by improper access to workplace medical records. Current federal law, such as the Americans with Disabilities Act (ADA), are inadequate in scope. For example, the medical record confidentiality requirements in the ADA go no further than requiring the medical record to be kept in a separate file. The ADA does not address who has access or when access is permitted.

Occupational physicians and other workplace health care providers depend on the individual to completely and truthfully disclose private information before rendering a professional opinion. An employee must feel secure that the physician will treat their private disclosures in a dignified and confidential manner. The physician should disclose information received in confidence only in narrowly defined circumstances and only when it is in the best interests of the individual.

Employers may require access to personal information when considering requests for job accommodations, addressing threats to health or safety, or reviewing claims for workers' compensation benefits. Additionally, employers shoulder an increasing responsibility for providing other types of benefits and obligations, such as health and disability insurance, family medical leave, and employee assistance programs. As a result, the employer becomes inextricably and unavoidably involved in employees' personal and medical affairs.

Thus, competing interests between a worker's desire for privacy and the employer's legitimate interest in the health of workers create sensitive ethical and legal dilemmas for physicians in occupational medicine. Difficult ethical problems arise when attempting to balance the importance of the worker's need and right to keep medical information confidential versus the employer's need to know.

Occupational physicians acknowledge the importance of medical confidentiality in the College's Code of Ethical Conduct. The code includes the following:

"5. keep confidential all individual medical information. Releasing such information only when required by law or overriding public health considerations, or to other physicians according to accepted medical practice, or to others at the request of the individual"; and

"6. recognize that employers may be entitled to counsel about an individual's medical work fitness, but not to diagnosis or specific details, except in compliance with laws and regulations."

ACOEM recognizes its Code of Ethical Conduct to be the standard of conduct expected from those providing occupational medical services. However, the College believes that additional guidance by legislation is necessary to protect the worker's expectation for confidentiality and to give the physician's ethical responsibility the force of law.

Secretary Shalala's recommendations for workplace protections are too narrowly crafted. The Secretary recommends that employers not be "controlled by the legislation," but be considered health care providers or payers when they actually perform those activities and "be obliged to conduct themselves accordingly."

The College recommends that comprehensive federal legislation reflect the following principals:

1. Physicians should disclose their professional opinion to both the employer and the worker when the worker has undergone a medical assessment for fitness to perform a specific job; however, the physician should not be required to give the employer specific details or diagnoses unless the worker has authorized the disclosure.

2. Supervisors and managers may be informed by the physician regarding necessary restrictions on the work or duties of the employee and recommended accommodations. However, the physician should not provide, or be coerced to provide, the medical information on which the restriction or accommodation is based.
3. Physicians should recognize a consent for disclosure only if the consent is informed and is made without duress.
4. Physicians should be a source of professional, unbiased, and expert opinion in the workers' compensation or court systems, and should only disclose medical information that is relevant and necessary to the claim or suit. The decision on disclosure of relevant and necessary medical information should be solely that of the physician.
5. The physician should develop a written policy for the treatment of medical records in their offices, clinics or workplaces. The policy should address such issues as where and how medical records are stored; the security of medical records, including medical databases; what happens in the event of employee resignation, layoff, termination, job transfer, or plant closure; and the mechanisms of employee access and consent for disclosure.
6. Although workplace medical records may be considered the property of the employer, this ownership does not abrogate any of the principles of confidentiality. However, the custodian of the record should always be the physician or responsible health care provider and access to the record should be controlled by the custodian. The medical record captures the confidentiality of communications within the patient-physician relationship. For the physician to provide the best and most appropriate medical care, a worker must feel that they can disclose to their physicians personal facts and information that they may not want others to know. Access by corporate officials, e.g., employee relations, in-house legal departments, and other functions, should proceed via the physician and in accordance with procedures for disclosure.

ACOEM urges the Congress to enact comprehensive federal medical records confidentiality legislation that encompasses protection of an individual's personally-identifiable medical information in all settings, including the workplace.

Washington Contact: Pat O'Connor (202–223–6222)

Statement of American Hospital Association

The American Hospital Association (AHA) represents the nation's 5,000 hospitals, health care systems, networks and other providers of care. We appreciate this opportunity to present our views on an issue of great importance to our members and the patients we serve: protecting the confidentiality of private health care information.

As health care providers, AHA members are deeply involved in both the use of private health information, and in ensuring that the information remains confidential. Our comments reflect our members' experiences and needs in balancing these two important issues.

Protecting the Trust Between Providers and Patients

Every day, thousands of Americans walk through the doors of America's hospitals. Each and every one of them provides care givers information of the most intimate nature. They provide this information under the assumption that it will remain confidential. It is critical that this trust be maintained. Otherwise, patients may be less forthcoming with information about their conditions and needs—information that is essential for physicians and other care givers to know in order to keep people well, ease pain, and treat and cure illness.

If care givers were not able to obtain and share patients' medical histories, test results, physician observations, and other important information, patients would not receive the most appropriate, high-quality care possible.

Our members consider themselves guardians of this information, which is why AHA has long supported the passage of strong federal legislation to establish uniform national standards for all who use health information. We were pleased that the Health Insurance Portability and Accountability Act (HIPAA) of 1996 pushed this issue to the forefront by requiring the Secretary of Health and Human Services to issue recommendations to Congress on this important topic. We commend Con-

gress and this committee for taking up the difficult task of balancing the needs in this area.

It's an issue that affects each of us personally. We live in a time of rapidly advancing technological improvement, when the world seems to get smaller as computers get more powerful and databases get bigger. This technological change can be positive—it has led to significant improvements for both health care providers and their patients—but it worries people who are justifiably concerned about how information about them will be used.

In health care, we must take the steps necessary to protect that information from those who would misuse it. We need strong, uniform federal legislation to do it.

AHA Goals For Legislation

First and foremost, because we as hospitals and health systems put our patients first, we must restore people's trust in the privacy and confidentiality of their personal health information. Federal legislation can do this by establishing a uniform national standard for the protection of health information—including genetic information—a standard that balances patient privacy with the need for information to flow freely among health care providers. The AHA believes that federal confidentiality legislation must meet the following goals:

Allow patients and enrollees access to their medical information, including the opportunity, if practical, to inspect, copy, and, where appropriate, add to the medical record.

Patients have a right to know what information is in their records. This level of accountability encourages accuracy and has the added benefit of encouraging patient involvement in their care. It is not appropriate for patients or enrollees to request deletions from their records even if the information is incorrect. Medical or claims decisions may have been made based on that erroneous information and it should be left in the record to ensure accuracy for future users. Any amendments or corrections should be added to the original information.

Preempt state laws that relate to health care confidentiality and privacy rights, with the exception of some public health laws.

Health care today is delivered through providers that are linked across delivery settings, and through organizations that cross state boundaries. AHA believes that the best way to set important standards for confidentiality of health information is to do so uniformly—through a strong federal law. This law must be both a floor and a ceiling, preempting all state laws with which it may conflict, weaker or stronger. Only through such a uniform law can patients' confidential information be equally protected regardless of the state in which they live or travel.

Be broad in its application, covering all who generate, store, transmit or use individually identifiable health information, including but not limited to providers, payers, vendors, and employers.

Patient confidentiality cannot be ensured unless standards are applied to all who may have access to health information. Legislation should cover all types of individually identifiable health information, including sensitive issues such as substance abuse, mental health, and genetic information.

Because of our strong belief in this concept, the AHA has been very concerned about model privacy regulation that is being developed at the National Association of Insurance Commissioners (NAIC) and would apply only to insurance carriers. This attempt to address enrollee privacy concerns through insurers potentially expands the ability of insurers to use individually identifiable information by expanding insurer responsibility into areas that are more appropriate for providers. The model holds insurers responsible for amending patient records and establishing Institutional Review Boards (IRBs) for research. It also holds insurers responsible for making sure that providers with whom they contract have confidentiality and security policies that are "substantially similar" to their own. This limited approach illustrates the problems with addressing this problem in a piecemeal manner.

Strike an appropriate balance between patient confidentiality and the need to share clinical information among the many physicians, hospitals and other care givers involved in patient care.

Care is increasingly provided by groups and systems of providers as opposed to individual providers. These new systems create opportunities for real improvements, but they rely heavily on a free flow of information among providers. Patient confidentiality is of the utmost importance. But in order to ensure that care is coordi-

nated and the patient's experience is as seamless as possible, information must be accessible to all providers who treat the patient.

To ensure this smooth coordination of care, the AHA supports legislation that requires a health plan to obtain from its enrollees authorization for the entire range of treatment activities that could be needed. Providers should still be allowed to ask for other authorizations—for example, if a patient is to receive sensitive tests or procedures that might require the provider to consult with others during a course of treatment. But, because it is impossible to know in advance all the different practitioners who might be involved in a single health care case, multiple levels of authorization would create unscalable barriers to the smooth coordination of care.

Another important issue is how to make sure providers have all the information they need to treat the patient. Some proposals allow patients to decide which providers can and cannot have access to their records, and what information the provider can and cannot see. While we understand the concerns of patients who want to limit the amount of information in their records that is made available to providers or payers, we believe strongly that decisions about what information is necessary must be made by trained health personnel. At the same time, however, information that is requested by a provider or payer must be clearly related to the purpose for which it is disclosed.

Recognize that a hierarchy of need exists among users of health information.

While access to individually identifiable information is essential for patient care, it may also be necessary for provider and health care system efforts to measure and improve the quality of care they deliver.

To limit its potential misuse, all within the health system should restrict the availability of individually identifiable information. Technology is available to do this, through encryption, audit trails, and password protection, for example. Another method for restricting the availability of individually identifiable information is to aggregate information whenever possible. Patients should be assured that unique, identifiable information about them is available for their treatment, but that its availability for other uses is tightly controlled.

Specific guidelines should be established to control the disclosure of individually identifiable information to various categories of users, including law enforcement officials, researchers, and employers.

Regarding law enforcement, the AHA believes that leaving in place current state laws—as recommended by the secretary of HHS—would set a dangerous precedent. Inconsistencies in these laws could allow local law enforcement agencies unrestricted access to confidential patient records, and free rein to re-disclose the information contained in them. Federal safeguards need to be put in place that ensure patient information is provided only when truly necessary—and that its subsequent use is tightly controlled. Such decisions should be left to a neutral magistrate, from whom law enforcement agents must request a warrant or subpoena to obtain individually identifiable patient information.

In the area of research, it is critical that legislative proposals distinguish between—on the one hand—human subject research under an IRB and non-intervention medical records research involving no contact with patients, and—on the other hand—the internal operations that a hospital or health system undertakes to improve care. For example, many institutions use individual medical records to track outcomes and conduct case and disease management. Confidentiality legislation should recognize that these activities are not research, but activities integral to the basic function of a hospital or health system—continually striving to improve the health care they deliver.

When individually identifiable information is used by employers, two things are critical: the employer must have access only to information needed for the functions it may perform as an ERISA health plan—treatment, payment or administration; and this private information must be available only to those who administer the health plan.

Include sufficient civil and criminal penalties to deter inappropriate disclosure of individually identifiable information.

The level of these sanctions should vary according to the severity of the violation. At the same time, any penalty imposed must take into account good-faith efforts by providers who establish data safeguards, educate employees about complying with the safeguards, and attempt to maintain secure record-keeping systems.

Conclusion

The smooth exchange of patient information is critical to providers and patients alike as our nation's health system rapidly becomes more integrated. We need federal legislation to protect this sensitive information from being misused. The AHA looks forward to working with you to develop legislation that, by adhering to the goals stated above, protects patient confidentiality, does not get in the way of high-quality health care delivery, and is truly a uniform national standard.

Statement of Healthcare Leadership Council

The Healthcare Leadership Council (HLC) a trade association representing all sectors of the health care industry, including pharmaceutical companies, hospitals, managed care, providers and device manufacturers, submits the following statement regarding patient confidentiality for the record created in response to the March 24 hearing held by the House Committee on Ways and Means, Health Subcommittee. The HLC members are the innovators in the health care industry, and share a commitment to a consumer-focused health care system and a dedication to providing high quality health care services to every patient. Information is the cornerstone of innovation and quality. It serves as the basis for the knowledge we need to serve, treat, counsel, prescribe therapies, and reimburse patients, and to discover how all of these activities can be done better and more effectively. Without efficient access to information, the evolving health care delivery system will come to a grinding halt, and consumers will be denied the real-world benefits of all that the health care industry has to offer today and well into the future.

The HLC supports the passage of federal confidentiality legislation, while assuring the appropriate information sharing needed by network-based health plans, researchers and purchasers to provide high quality affordable care for consumers. We applaud the recent Ways and Means Health Subcommittee hearing. The issues discussed will help build a strong foundation for the upcoming debate Congress will have on this most important issue. We appreciate the inclusion of our statement in the record.

For more than two years, the HLC has been engaging in an earnest effort to work with its members and others in the industry to craft workable and meaningful confidentiality protections that provide important confidentiality assurances to the patient while at the same time allowing health plans, providers and health product manufacturers to use patient health information for purposes that are necessary and appropriate to the provision of high quality health care services.

In searching for a workable federal legislative solution, the HLC has identified the following principles as necessary to striking the right balance between the patient and the information needs of the health care industry. These basic principles are as follows:

(1) Support for federal standards regarding the confidentiality of all patient health information; (2) Application of standards only to identifiable health information, leaving non-identifiable health information (*i.e.*, coded and encrypted data) available for use in research and for other health-related purposes; (3) Treatment of all identifiable patient health information, including genetic information, the same way to assure the same strong confidentiality protections; (4) Facilitation of appropriate uses and sharing of patient health information with recognition that access to information is not harmful, but rather helpful to the patient; and (5) Provision for strong and thorough preemption of state law.

1. Federal standards. Federal standards ensuring the confidentiality of patient health information are critical to guaranteeing the uniform, consistent treatment of such information throughout the country. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) took important steps in the right direction by requiring that a standardized information transmission and storage system be developed, and that such systems be kept secure. In addition, HIPAA mandates that Congress enact federal confidentiality standards by August of 1999. Failure to do so will trigger Secretarial authority to promulgate regulations guaranteeing such protections within six months.

The time has come for a uniform federal standard. The HLC supports federal standards regarding disclosure and use of an individual's identifiable health information, for safeguarding the confidentiality of that information, and for establishing an individual's rights to inspect and copy his or her records. A uniform standard is the only way to avoid a dual-regulatory environment. State authority should remain paramount over areas of confidentiality that do not conflict with national uni-

formity and consistency, such as state reporting requirements for public health and safety dangers and licensure of providers.

2. Treat all identifiable health information in the same manner. The HLC supports extending strong and consistent confidentiality protections to all personally identifiable patient health information. As such, the HLC is concerned about recent proposals, such as that introduced by Rep. Slaughter (D–NY) (H.R. 306), to treat genetic information separately from other patient health information. As a practical matter, it would be difficult if not impossible for health plans and providers to treat and secure genetic information differently than other patient health information as almost all health information contains an important genetic component. How then can we elevate certain types of health information to a higher status more deserving of protection than other information? All personally identifiable patient health information should receive the same strong protections against inappropriate disclosure.

3. Scope of federal standards should apply to individually identifiable information only. In its effort to craft federal confidentiality standards, Congress should apply these protections to individually identifiable health information only where there is a legitimate need for confidentiality. The current trend is toward anonymizing information—that is, rendering the information available but leaving the identity of the subject individual unknown—and a more narrow focus on individually identifiable health information would provide an important incentive to encrypt, encode and otherwise anonymize patient health information wherever possible.

The HLC strongly believes that any federal confidentiality standards should provide incentives for health plans, providers, purchasers and other product manufacturers to continue using *non-identifiable* health data to make advancements, cure diseases and study the effects of new treatments. Allowing the use of anonymized health data directly facilitates health research and limiting its use would stifle the phenomenal medical advances being made almost daily in this country. To further ensure the confidentiality of patient health information, however, the HLC strongly supports subjecting any "encryption key" or other such code used to anonymize information to the same strong protections provider for other protected, identifiable health information.

4. Provide for appropriate health information sharing with confidentiality protections. Any federal confidentiality standards adopted by Congress must adequately and effectively recognize that most health care services are delivered through some form of integrated delivery system. This modern health care system, which is marked by a team-approach to health care delivery, relies heavily on information sharing and collaboration to ensure high quality services are provided to the patient. As a result, it is crucial that strong patient confidentiality protections allow and facilitate appropriate information sharing to further this goal. Following are several key points explaining the HLC's perspective:

- An integrated health care delivery system requires more information sharing. Only in focusing on what are and are not appropriate "uses" of patient health information can we develop confidentiality protections that effectively distinguish between what is helpful and harmful to the patient and to consumers generally. Our health care delivery system is no longer one defined by discrete encounters with a number of different and unrelated physicians and providers. Rather, the current delivery system is distinguished by a growing number of innovative arrangements between and among physicians, health plans, employers, hospitals and researchers. We now have teams of professionals responsible for coordinating the health care services provided to patients. These teams involve multiple individuals, including physicians, nurses, lab technicians, pharmaceutical manufacturers and others. Together, these varied participants are working in the interest of the patient.

As a result of these important improvements in the health care delivery system, the HLC supports establishing strong confidentiality protections consistent with the direction of our delivery system. Specifically, the HLC supports allowing the use of patient information for purposes of providing treatment, securing payment, conducting health care research and undertaking quality assurance activities. These activities are all designed to benefit the consumer.

Medical records research is vital to maintaining and improving the health of the American public. In fact, virtually every health hazard that we know of today has been identified using information from medical records. Take AIDS, for example. If researchers had not been allowed to study the medical records of patients with unusual immune deficiency problems in the late 1970's, the characterization of the AIDS epidemic would have been delayed at substantial cost to the public's health. Other examples include studies examining the benefits and risks of estrogen treatment, the health risks of: smoking, dietary fats, obesity, and certain occupations; infectious disease studies which led to the development of vaccines for polio, measles

and other infectious diseases; and studies which show the effect of breast cancer screening programs.

Another example is the outbreak of "flesh eating strep" identified at the Mayo Clinic in 1996. Without access to the medical records of patients with these unusual infections, characterization of this syndrome and isolation of this deadly bacterial strain would have been delayed. And over a hundred school children—which the Mayo research showed were the unwitting carriers of this deadly germ in their throats—would have gone untreated. Every medical advance mentioned here has relied heavily on information from patients' medical records. Without access to this rich source of clinical information, many of these advances simply would not have occurred.

- You can't expect a surgeon to operate blind. Legislation must emphasize confidentiality and provide strong disincentives for abuses of information; however, the HLC is concerned over recent proposals that would appear to place the patient in a position of having ultimate veto power over access to information. To put patients, who by and large rely on lay knowledge, in a position of deciding whether to grant access of information to some and not to others ultimately puts them at risk. Again, federal standards should focus on the appropriateness of information disclosure and its use.
- The move toward electronic transmission of information brings forth tremendous benefits for the patient, but also creates fears. The Health Insurance Portability and Accountability Act (HIPAA) will result in numerous standards regarding the security of electronically transmitted information. The concept of a unified medical record is revolutionary in the benefits that will inure to patients. There will be fewer adverse drug reactions, fewer mistakes made and fewer unintended consequences. Electronic data storage presents a greater opportunity to secure information than in the current system of open file cabinets, etc. At the same time, anything new and unfamiliar can cause trepidation. It is the fear of the unknown. Yet a unified medical record stored electronically actually can keep information more secure than paper copies in files, as mentioned before. Computer records can be safeguarded through encryption, password access and other similar technologies.
- The HLC is concerned over efforts to use the confidentiality debate to advance other agendas, such as anti-managed care and insurance product pricing issues. The HLC grows increasingly concerned that the debate over how to keep patient health information confidential in the current health care delivery environment is becoming a vehicle for debate regarding the delivery system as a whole. Again, the HLC advocates responsible and appropriate information sharing and use. However, any debate desired about such practices as medical underwriting, utilization review/utilization management and other quality assurance techniques should be held separately and should be dealt with on the basis of their merits. The HLC caution's Congress against effectively putting an end to such practices through the guise of protecting the confidentiality of patient information.
- Confidentiality protections are already in place. Health plans and providers submit to voluntary accreditation, which includes evidence of strong confidentiality protections. For example, the National Committee for Quality Assurance (NCQA) and the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) are two accrediting bodies which require health plans and hospitals to have written confidentiality policies and procedures in place, to take action at patient care sites to guard against unauthorized or inadvertent disclosure of confidential information, and to obtain patient consent for information release. In addition, the Federal Privacy Act imposes numerous confidentiality requirements on health plans and providers participating in the Medicare program. Similarly, the Institutional Review Board (IRB) process involving clinical research holds pharmaceutical manufacturers, device manufacturers and other researchers to stringent confidentiality standards.

5. Strong federal preemption of state law. The HLC strongly supports effective federal confidentiality protections for consumers as long as the standards include strong and thorough preemption of state law in those areas in which the federal government has legislated. Without adequate preemption, providers, health plans, purchasers and manufacturers would essentially be subject to 52 different confidentiality laws, which is unworkable and leaves consumers vulnerable under a patchwork of protections.

CONCLUSION

With these important HLC principles in mind, we are concerned that current legislative proposals fail to recognize that most health care services today are delivered in some integrated delivery context. Any legislative restrictions limiting access to medical records threaten our ability to engage in quality-enhancing activities as well

as the very existence of entire categories of medical research. In addition, we are concerned about proposals that would require that we obtain patient authorization each time patient information is used. This could result in a patient's ability to revoke authorization to use information to provide essential services, as well as undermine research. This is because individuals who deny consent are systematically different in important ways from individuals who do consent. For example, individuals who deny consent may have had worse outcomes or they may be less satisfied with their care.

Studies describing the outcomes of diseases or the effectiveness or cost-effectiveness of treatments which exclude such individuals would be biased—they give us the wrong answer. Moreover, while research is clear on the point that individuals who deny consent are systematically different from those who consent, the direction and magnitude of those differences are completely unpredictable from study to study. So not only will such research result in the wrong answers, but it will be impossible to determine how wrong they are or in what way. Thus, the reliability and validity of findings from such research will be suspect and lead to the design of potentially incorrect medical treatments. The inclusion of all qualifying individuals is the only way to assure that accurate conclusions are drawn about the prognosis of disease, the outcomes of therapy or the quality of care.

The underlying motivation for many of the legislative proposals is to keep personal medical information between the patient and his or her physician. While this idea could be very attractive; in our complex health care environment, it is an unattainable ideal. For example, in an average medical visit the following individuals and groups have access to a patient's complete medical record: the appointment office, the registration desk, all physicians, physician assistants, and nurses who provide care for the patient as well as their receptionists and secretaries, all laboratory, EKG, and x-ray technicians who perform the necessary tests, infection control officers who regularly survey medical records for reportable diseases, continuous improvement staff who strike to improve out health care processes, members of the marketing department who seek to ensure patient satisfaction, the business office for billing, the legal department, and insurers and other third-party payers.

With this in mind, the Healthcare Leadership Council would like to work with lawmakers in search of meaningful and balanced federal confidentiality standards that allow us to achieve the promise of the information-based 21st Century health care delivery system. The HLC looks forward to working with you and your staff.

Thank you for your attention and leadership on this most important issue.

INTERNATIONAL SOCIETY FOR
PHARMACOEPIDEMIOLOGY
2000 L Street NW., Suite 200
WASHINGTON, DC 20036

March 25, 1998

The Honorable Bill Archer
Chairman, House Ways and Means Committee
Attention: Bradley Schrieber
Room: 1102 LHOB
Washington, DC 20515

RE: Written Testimony on Medical Confidentiality, March 26, 1998 Hearing

Dear Mr. Chairman:

On behalf of the International Society for Pharmacoepidemiology (ISPE), we are pleased to submit written testimony in response to the hearing regarding the confidentiality of medical records and draft legislation scheduled for March 26, 1998. Our professional society embraces the principle of protecting the confidentiality of individually identifiable medical information while preserving justified research access to such information in the interest of the public's health.

The research conducted by members of our society and others in our field evaluates populations to understand the extent, natural course, and burden of diseases. Pharmacoepidemiology is an observational, non-experimental science. In contrast to clinical trials, which are experimental, an epidemiologic observational study observes patients in the real world of clinical medicine, and the patient is at no medical risk from being part of the study. It is the science of pharmacoepidemiology that is used to evaluate the risks and benefits of medications in large numbers of pa-

tients in the real world setting. Pharmacoepidemiologic studies have had a major impact on the public's health in general and on our understanding of the risks and benefits of medications in particular. For example, such studies documented the risk of aspirin and Reye's Syndrome in children and the risk of vaginal cancer in daughters of women who took diethylstilbestrol (DES) while pregnant. Pharmacoepidemiologic studies will continue to be important in the future. ISPE urges that any new laws or changes in existing laws aimed at further protecting data privacy be formulated with an acknowledgment of the value to society of pharmacoepidemiologic research.

We are especially concerned about legislation relating to patient informed consent and the use of IRBs for certain observational research that uses encrypted patient data, and we pay special attention to the definition of "identifiable data." While the development of new legislation presents an opportunity to strike a fair balance between individual privacy needs and legitimate access to information for research in the public's interest, there is also the opportunity to inadvertently stifle important research, while offering no meaningful new protections. We offer our help to you, your colleagues and your staff in the development of legislative answers to these important and complex issues.

Yours sincerely,

JEROME L. AVORN, M.D.
President

ELIZABETH ANDREWS, PH.D.
Chair, Ad Hoc Committee on Data Privacy in the US and Canada

Enclosures

International Society for Pharmacoepidemiology ISPE Fact Sheet 1997–98

MEMBERSHIP

More than 1300 members from 45 countries
- Pharmaceutical Industry—35.6%
- Academic Institutions—40.8%
- Government Agencies—11.0%
- Clinical Practice & Consulting—12.6%
- North America—50.1%
- Europe—36.1%
- Asia—8.6%
- Other Continents—5.2%
- Correspondents in 19 Countries
- National Chapters in Argentina, Belgium, Netherlands
- Associate to Member of World Health Organization Council for International Organizations of Medical Sciences (CIOMS).

MEMBERSHIP BENEFITS

- Pharmacoepidemiologic Scientific Forums for Research Interchange
- Policy Fromulation Relevant to the Professional and Research Work
- Environments
- Enhanced Professional Communication:

—Forum Networking Opportunities
—Reduced Registration for Annual International Conference on Pharmacoepidemiology
—Subscription to the journal
—Reduced Subscription Price

Society Objectives

MISSION STATEMENT

The International Society for Pharmacoepidemology (ISPE) is a non-profit international professional membership organization dedicated to promoting pharmacoedpidemiology, the science which applies epidemiological approaches to studying the use, effectiveness, value and safety of pharmaceuticals. ISPE is firmly committed to providing an unbiased scientific forum to the views of all parties with interests in drug development, drug delivery, drug use, drug costs, and drug effects.

A. Establishment of scientific forums.

1. Convene an annual scientific forum where members of the discipline meet each other, present results of methodologic investigations and studies in progress, discuss public health policy issues concerning pharmacoepidemiology, etc.

2. Convene periodic symposia on scientific and public policy issues of common interest.

3. Sponsor industry, provider, and academic caucuses to address issues of particular interest to caucus members.

4. Convene periodic consensus conferences.

B. Dissemination of scholarly and practical information.

1. Publish a newsletter highlighting emerging issues, news of the field, employment opportunities, etc.

2. Collect information on existing curricula and aid in developing curricula criteria and professional training standards. Provide information on worldwide training opportunities.

3. Sponsor/co-sponsor/co-sponsor superior quality peer-reviewed publications.

A. Facilitation of professional communication.

1. Establish a clearinghouse on data resources for pharmacoedpidemiologic studies.

2. Establish a directory of pharmacoedpidemiology consultants.

A. Capacity building.

1. Establish funding resources for pharmacoepidemiology training scholarships.

2. Act as an advocate for the field in affecting health policy and the allocation of resources with government agencies, the pharmaceutical industry, private foundations, universities, other professional groups.

[Additional material is being held in the Committee files.]

Statement of Medical Group Management Association

Mr. Chairman and Members of the Subcommittee, the Medical Group Management Association (MGMA) appreciates this opportunity to provide input on the general issue of patient confidentiality. As this issue is further developed and legislation is crafted, MGMA will submit a more detailed analysis.

MGMA is the oldest and largest association representing physician group practices with more than 8,900 health care organizations nationwide in which just under 200,000 physicians practice medicine. MGMA's membership reflects the diversity of physician organizational structures today, including large tax-exempt integrated delivery systems, taxable multi-specialty clinics, small single specialty practices, hospital-based clinics, academic practice plans, integrated delivery systems, management services organizations, and physician practice management companies.

MGMA believes that the provider-patient bond is the most important relationship in the health care arena. Even with the changes occurring in the marketplace, the trust engendered in these encounters should remain constant. Physician practices have a duty to patients to ensure their medical records are held in confidence and are disclosed only in appropriate situations. The evolution of information flow, health care records computerization, managed care contracting, and organizational restructuring require an appropriate balance for health care systems to thrive while simultaneously safeguarding the confidentiality of medical records. The following represents MGMA's support of the highest level of medical records confidentiality that can be achieved without imposing onerous regulations on physician practices.

Applicability to Smaller Practices

Confidentiality policy should not be predicated on new personnel intensive statutes or regulations, at a time when pressures to contain costs are forcing physician offices and hospitals to decrease staffing. MGMA urges Congress and the Administration to consider how confidentiality legislation will impact physician practices. There is no cookie cutter process for all physician offices, and certain provisions, such as those that are technology-based, would disproportionately burden small practices.

Medical and Outcomes Research

Patient confidentiality legislation and regulations should not unnecessarily interfere with legitimate medical research. MGMA believes the confidentiality of medical records must be balanced against the benefits of medical research and efforts to improve the quality of care. Aggregating medical data, being able to access subjects' profiles, and possibly contacting subjects for follow-up information are vital components of medical research. Institutional review boards should be permitted to waive informed consent requirements for the minimum amount of necessary disclosure, when appropriate standards have been developed and have been applied to clinical and quality research initiatives by institutional review boards.

Scope of Statutes

Anyone who improperly discloses confidential medical records should face civil and criminal penalties. MGMA urges policy makers to adopt confidentiality measures that apply to *everyone*. Whether a health care provider improperly reveals information to an employer, or a person finds medical records and reveals them publicly (e.g., to a newspaper), an individual suffers both emotionally and financially when a person breaks a medical confidence.

National Standards

Policy makers should ensure that federal preemption is part of confidentiality legislation. Lawmakers should build in protections at the federal level to guard against specific types of disclosure and discrimination. This will ensure that *every* patient has the security of knowing that his or her records will remain confidential, and will allow providers with patients residing in different states to know how confidentiality standards apply to their practices. National uniformity will give physicians one set of standards and will make compliance feasible.

Notification Requirements

Notifying third parties of incorrect information within a medical record is a shared responsibility. Health care providers should notify those parties they have previously provided with unamended information of substantial changes to a patient's health records. In addition, if patients notify health care providers that third parties are in receipt of incorrect information, physicians should be responsible for notifying the identified party of changes which substantially alter the insurance risk for an individual or substantially affect the care rendered by another health care professional. In contrast, asking physician practices to become the hub of a notification cycle between contractors and others who may be in receipt of incorrect information imposes unwarranted regulatory burdens on physician practices.

Identifying Improper Disclosure

Statutes or regulations should define explicitly improper disclosure of medical records. Federal policy should carve out situations where disclosure is unlawful and attach appropriate penalties to identified improper disclosure. This contrasts with the assumption that all but narrowly defined disclosure is improper. MGMA believes that lawmakers can target prohibited behaviors without significantly hindering health care systems' operations or medical research by assuming the impropriety of information flow. As such, MGMA supports the approach taken in Representative Chris Shays' draft legislation, which would facilitate compliance with the statute, rather than presuming that all disclosure is improper.

Law Enforcement

Law enforcement access to medical records should be balanced against a patient's right to privacy. Much as medical records confidentiality should be balanced against the above factors, it should be considered in light of law enforcement needs. While MGMA acknowledges law enforcement's investigative needs, we believe that law enforcement access to records should not be unfettered. Health care providers should release medical records to law enforcement officials only when police or investiga-

tors have obtained a court order which protects the information from further disclosure.

In closing, we would like to thank the Subcommittee for its consideration of this issue and of MGMA's perspective. We will continue to provide comments as the confidentiality issue develops and appreciate the opportunity to comment on this issue.

For further information, please contact Rayna L. Richardson, Government Affairs Representative, at (202) 293–3450.

Statement of National Breast Cancer Coalition

Thank you, Mr. Chairman and members of the Committee for your leadership efforts to begin to address the important issues of patient protection and the advancement of medical research inherent in the medical privacy discussion as we move into a new era of research and information technology.

The National Breast Cancer Coalition (NBCC) is a grassroots advocacy organization dedicated to eradicating breast cancer. We are made up of 400 member organizations and hundreds of thousands of individuals. The NBCC seeks to increase the influence of breast cancer survivors and other activists over research, clinical trials, and public policy and to ensure access to quality health care for all women.

It is critical that as the nation begins to address issues of medical privacy, we also address issues of genetic discrimination. The NBCC strongly believes federal legislation is needed to establish a national policy which ensures confidentiality; protects individuals from genetic discrimination; controls the use of health information collected by health care payers and providers; requires authorization for the use of an individual's health information for other purposes; and does not impede the progress of biomedical, behavioral, epidemiological and health services research. We believe medical research should be encouraged and pursued—but in a way that protects the rights of individuals and enhances public trust in medical research. We want to work together with policy makers and the scientific community to strike the appropriate balance between the protection of individual privacy rights and the pursuit of biomedical research.

The NBCC believes individual privacy rights are fundamental to being a citizen in this country. As breast cancer survivors, we believe that our illness, diagnosis, treatment and prognosis is very personal and intimate information. It is paramount to NBCC, that individuals have the right to decide to whom and under what circumstances their protected health information, including genetic information, will be disclosed and the right to inspect and copy their own medical records.

In addition, the NBCC believes medical privacy and discrimination around genetic testing are related issues which must be addressed simultaneously. Genetic discrimination issues drive many of the underlying medical privacy concerns, so to try to regulate medical privacy without confronting issues of genetic discrimination is ludicrous. For example, to ensure protection against genetic discrimination, individuals should be able to segregate certain private information to be filed separately so it will not be distributed to health care payers with the rest of the patient's chart. Breast cancer patients should be able to request that genetic information such as BRCA 1 and BRCA 2 test results are not sent to insurers or others, but are sent to the radiologist to ensure the results of a mammogram are read accordingly.

The misuse of medical information must stop. We do not want to wake up like we did earlier this year to front-page newspaper stories about major pharmacies selling medical records to marketing firms without authorization. Nor should we be fearful of talking frankly with our physicians about our medical conditions because the information may end up in the wrong hands or cost us our health insurance or jobs. The increasing complexity of the current information age demands a public solution to protect our rights to privacy. Federal legislation must be enacted which will safeguard our privacy, prohibit the unauthorized disclosure of protected health information (except under very limited exceptions) and protect an individual's personally identified health information from misuse.

We need protection against the improper use and unauthorized disclosure of genetic information. Everyone cheered the discovery of the breast cancer genes, BRCA 1 and BRCA 2, but if we are ever going to have the knowledge for this discovery to make a difference in eradicating breast cancer we must limit disclosure of genetic information and outlaw genetic discrimination in health insurance and the workplace. Such disclosure can cause significant harm to individuals, including stigmatization and discrimination by health insurers and employers. At the very least, the NBCC believes that an entity should be prohibited from disclosing genetic infor-

mation without the prior written authorization of the individual. We also believe legislation should include prohibitions against discrimination by employers, making it unlawful to refuse to hire, to discharge, or to deprive individuals of employment opportunities based on genetic information, including an individual's request for genetic services. It should also extend such protections against genetic discrimination to health insurance and prohibit health plans from denying, canceling, refusing to renew, or changing the terms, premiums or conditions based on genetic information.

In addition, federal legislation must limit authorization for disclosure of protected health information only to what is necessary for the provision of treatment and payment services. The ability of insurance companies to share medical information throughout its other divisions is a direct threat to the privacy and protection of medical records. Most insurance companies are complex financial institutions. Without protection, the same company that pays for health care would be able to share medical information across divisions, such as life insurance, financial planning, disability, etc. We believe there should be strong criminal and civil penalties for intentionally or negligently using individually identifiable health information and individuals should have a civil right of action against anyone who misuses their protected health information.

A critical piece to protecting medical information is informed consent. But informed consent today affords little, if any, protection. These documents are rarely read because of their length and legal terminology. As patients seeking medical care, we have to sign blanket waivers allowing disclosure of our medical information in order to obtain treatment or payment for care. These authorizations do not protect us as they should from unnecessary disclosure because we have no idea how the information will be used. Women sign these documents because they think their signature is necessary to receive vital health care. The NBCC believes that any authorization should be limited to treatment services and payment purposes and that the definition of information that can be provided be construed as narrowly as possible. A legal obligation of confidentiality should be imposed on those who provide and pay for health care, as well as on the entities that receive that health information.

Securing medical privacy rights, however, should not come at the expense of medical research. Despite our best efforts and your leadership, breast cancer is still the most common form of cancer in women. We still do not know the cause or have a cure for this dreaded disease. Over the past few years, there have been incredible discoveries at a very rapid rate that offer fascinating insights into the biology of breast cancer, such as the isolation of breast cancer susceptibility genes and discoveries about the basic mechanisms of cancer cells. These discoveries have brought into sharp focus some of the areas of research that hold promise.

The NBCC believes that legislation protecting medical information and privacy should be balanced. We want to see federal standards that safeguard personal health information while protecting the ability of researchers to conduct vital biomedical research. We don't believe that you can have one without the other. Knowledge about how to prevent and cure breast cancer will only come if women participate in research. But without appropriate safeguards against misuse, public distrust will increase and few women will be willing to participate in research efforts, whether donating tissue or enrolling in clinical trials. Women will have the confidence to participate in clinical trials only if they believe that their individual health information will be kept private so that it can't be used against them by insurers or employers. In addition, without a guarantee of privacy, women are less likely to be honest with their doctors, endangering their own health and slowing the overall progress of improved health care for the general population. It can't be emphasized enough that we must focus our attention on building public trust. There has to be real, believable protection if women are to place their trust in the medical and research process.

The NBCC would like to see the common rule protections extended beyond research funded by the National Institutes of Health. The NBCC believes these protections should be the same for all medical research whether publicly or privately funded. Much benefit to research could be obtained by giving research special privacy considerations. It may make it easier to distinguish research access from clinical chart access.

The NBCC believes that ideally there should be one federal statue that effectively guarantees privacy rights, but given the reality, we think it is advisable that federal legislation be seen as the floor; and that states should be able to pass laws that allow more stringent safeguards that do not, at the same time, inhibit medical research from going forward.

Mr. Chairman, and members of the Committee, thank you again for your leadership on this important issue. We look forward to working with you to restore public

confidence and trust in our medical system, and to achieve the necessary balance between individual privacy and the promise of medical research.

Statement of National Pressure Ulcer Advisory Panel, Alexandria, Virginia, Rita Frantz

I. INTRODUCTION

My name is Rita Frantz and I am the current President of the National Pressure Ulcer Advisory Panel. I am also a Professor at the College of Nursing at the University of Iowa. I am submitting this testimony on behalf of the National Pressure Ulcer Advisory Panel (NPUAP). The NPUAP appreciates the opportunity to provide written comments for the record regarding patient confidentiality.

The NPUAP is an independent, not-for-profit organization dedicated to the prevention and management of pressure ulcers. Formed in 1987, the NPUAP is comprised of fifteen leading authorities, representing various disciplines, including medicine, nursing, research, physical therapy and education—all of whom share a commitment to the prevention and management of pressure ulcers. The NPUAP serves as a resource to health care professionals and, while not a membership organization, welcomes and encourages the participation of those interested in the pressure ulcer issues through utilization of NPUAP educational materials, participation at national conferences, and support of NPUAP efforts in education, public policy and research.

Our organization was instrumental in developing the medical criteria and utilization parameters adopted by the Durable Medical Equipment Regional Carriers. Moreover, our panel members developed a definition and staging system for pressure ulcers. The Agency for Health Care Policy and Research used these guidelines when they developed their publication, "Pressure Ulcers in Adults: Prediction and Prevention."

The goal of the NPUAP is to assist health care professionals in reducing the incidence of pressure ulcers by 50%. In order to achieve this goal, our panel members, independent of the NPUAP, conduct extensive clinical trials and research. The impending patient confidentiality issue greatly impacts the clinical trials and research of our members. The NPUAP supports respecting and preserving patient confidentiality. There is a need for enforcing privacy in medical records. Any privacy initiatives, however, should not be so restrictive as to hamper quality assurance, vital health care research and education.

Specifically, NPUAP is concerned that while protecting a patient's rights to privacy, Congress's actions may inadvertently harm the interests of patients by unnecessarily restricting access to information needed by researchers and clinicians to (1) determine the safety and effectiveness of medical treatments, (2) assess the usefulness of diagnostic tests, (3) identify disease risk factors, (4) monitor the cost effectiveness of new interventions, (5) educate those entering the medical profession, and (6) ensure quality assurance/improvements. Such information is necessary to continue providing the public with health care.

II. AUTHORIZATION

The first issue of concern for the NPUAP regards proposed language that requires authorization every time a patient's record is accessed. The NPUAP agrees that patient authorization is necessary. We believe that a patient's authorization should be required in order to use a patient's medical record for a clinical or chart review study before beginning to conduct the study. However, we believe that only one authorization is necessary per study. If the focus of the study changes a new authorization should be sought. Requiring authorization every time the patient's record is accessed will greatly impact quality assurance, research and development and clinical trials as discussed in more detail below.

Quality Assurance

Quality assurance is required by JCAHO in every care setting that it accredits. Some state health departments or licensing agencies also require quality assurance activities in all nursing homes and home health agencies. Quality assurance is a standard of care. Most quality assurance activities involve chart review or collecting clinical information to improve the quality or delivery of care. Requiring patient authorization for every quality assurance activity would dramatically affect quality assurance efforts due to substantial burdens on time and labor. Furthermore, restrict-

ing data as inputs to quantitative studies minimizes the statistical significance of the resulting conclusions.

Quality improvement review of a patient's record requiring authorization would exclude many patients who are demented or confused and who do not have a legal guardian. These are the very patients for whom this kind of research is important. If we are unable to collect data on them because of the lack of a legally appointed guardian, a large number of patients will be omitted from studies.

Chart review studies within facilities designed to monitor quality of care, track outcomes, provide data to develop critical pathways or improve care are not truly "Institutional Review Board (IRB) reviewed studies." They also do not fit into the category of "treatment or payment" as defined in the draft legislative proposals or in the Secretary's recommendations. This access to medical records is an important quality improvement mechanism. Currently, there is no authorization requirement if the chart review is for quality assurance purposes. There should not be additional safeguards placed on facilities monitoring quality assurance or improvement. The NPUAP believes that quality assurance monitoring or studies should be excluded from any new or additional requirements.

If the study is an IRB reviewed study, upon obtaining informed consent, the IRB must approve the chart review process. Technically, this requires re-review for any new survey questions or tests that may be added on as an after thought. If the data gathered is from a previous chart review and it will be used for new or different analysis compared to the original study's intent, a new consent is required. For example, if a chart is reviewed to determine risk factors for pressure ulcers and later decide to re-analyze the same data and publish a paper on socio-economics, a new consent is required. The NPUAP supports the current IRB system and would like to see it maintained. IRB review is specifically designed to protect the rights of subjects, including the right of confidentiality.

Research and Clinical Trials

Innovations in medicine and medical technology continually revolutionize health care research. Continued progress depends on research and clinical trials. Frequently, the clinical trials and research involve collaboration with providers to study the safety of products utilized in clinical practice for treatment and prevention of pressure ulcers. In addition, results of research studies help design new clinical trials and monitor how well treatments work in clinical practice.

There is a requirement to obtain authorization for human subjects prior to enrolling them in a research study. All institutions that receive some type of federal funding must provide for review of research involving human subjects and must ensure that investigators obtain consent from subjects used in their research.

Chart review studies are a rich source for research. Many of the studies that the Agency for Health Care Policy and Research (AHCPR) panel used in the development of the "Guideline for Pressure Ulcer Treatment and Prevention" were either chart review studies or clinical trials that were built on information gained with pilot chart review studies. For example, much of what we know about risk factors for pressure ulcer development is based on chart review studies. Chart review studies are currently approved by IRB's without individual patient authorization provided confidentiality is maintained and there are no individual patient identifiers in the results.

In general the IRBs do a good job of reviewing each proposal on its own merits and helping to design a process that protects subjects confidentiality and safety, while trying to facilitate rather then block research. Each proposal is reviewed based on the overall risk to patients and the true need for the information. Therefore, in a clinical trial the patient expressly consents to the researcher's use of their medical information. As a result, the NPUAP does not believe that there is any need to require any further safeguards in this area. IRB monitored chart review research should continue without individual patient authorization...given the protective restrictions that currently apply.

III. ENCODING

The second topic NPUAP would like to address is the encoding issue. NPUAP believes that if patient identifiable information is used in research or clinical studies, it should be encoded: replacing identifying information by a code. The identity of the patient is not apparent from the information itself, but from the code issued.

If the patient's record is non-identifiable and the study contains no patient identifiable information, no consent is currently necessary. In this case, a medical record person, not connected with the study, makes a copy of the chart, goes through each page and blacks out any reference to patient identification. Non-identifiable patient

specific information is also information that has been aggregated in such a manner that the identities of the subjects can not be identified under any circumstances. Under these circumstances, the charts can be used for any purpose desired by the researcher. This process is extremely labor intensive and expensive. Non-identifiable patient informational data is generally not as useful for research as it lacks the detail that is required for meaningful or sophisticated analysis. A researcher could not recheck the chart or gather additional information for their particular study with non-identifiable patient information. A researcher could not notify the patient if they identified a problem in the patients care plan or treatment.

For clinical studies patient authorization documents should state that the researcher might need access to the patient's medical information for auditing and source verification. Furthermore, the authorization document should include a statement that the patient identifiable information will remain confidential. By signing the consent, the patient, or the patient's representative, has given their approval to review the medical record.

Once the authorization is obtained, patient's information becomes randomized. A subject number is assigned to a patient. This number is provided in an envelope, along with the treatment assigned by the clinical product number. The principal researcher then cites the subject number and their initials on each case report form for the patient. Only subject numbers are used in the data listings and subsequent reports. The identity of each patient can only be determined by the researcher. NPUAP believes this process for research is practical.

IV. Preemption

The NPUAP believes that the standards imposed by any legislative proposal should be universally applied. The NPUAP believes that there should be preemption of state laws. Uniform standards that preserve patient rights and that foster high quality clinical research efforts should be adopted.

V. Clarifications

In the Secretary's recommendations, and in some of the legislative drafts, there has been language suggesting that a patient can amend their medical record. It is unclear what type of amendments a patient would be permitted to make. If a patient is simply amending administrative items (address, phone number) that is acceptable. However, the NPUAP strongly disagrees with any language allowing a patient to amend medical or diagnosis information. The NPUAP believes that you should either prohibit a patient from amending their medical records or clarify this language to reflect what type of amendments a patient could make to their record. By not having this clarification and stating that a patient can amend their medical records, you imply they can amend their medical or diagnosis information. Besides the impending medical malpractice that would result, a patient should not be able to amend their medical information. NPUAP urges you to clarify the language so a patient is prohibited from amending any medical or diagnosis information contained in their medical record.

In the Secretary's recommendations and in drafted legislative proposals authorization is not required for disclosure of protected health information for payment purposes. It is unclear what is included in the term "payment purposes." If a provider of services were required to obtain a certificate of medical necessity, which includes patient identifiable information in order to be paid, would they be permitted to obtain the information without authorization?

A patient's record must be accessible to providers to the extent the information is needed to facilitate billing and care plan development. Failing to keep these records available could lead to duplication of services, missed diagnosis, and possibly abusive billing practices. Without the data required to establish medical necessity a provider would either not get paid or they could not successfully appeal any denials. The NPUAP believes a provider should be required to obtain a one time billing authorization. However, to require providers to obtain an authorization every-time a provider needed information for billing or appeals purposes would be a costly burden. The definition for "payment purposes" must be clarified.

VI. Conclusion

In summary, as your Subcommittee considers patient medical records privacy and confidentiality standards, the NPUAP implores you to remember how vital medical and records research is to maintaining and improving health care. Research on prevention, new treatments and products depends on patient's participation in clinical

trials and researcher's access to their relevant medical information as well patient databases.

Blanket signed authorizations allowing transfers of medical information to insurance companies, credit organizations, employers, etc. is problematic. This information can be either sold or transferred to national data banks where information may be used against the consumer or used for discriminatory purposes. This process should be stopped and medical information should be protected.

The NPUAP supports reasonable protections with appropriate safeguards. The NPUAP supports legislative language requiring patient authorization. However, we believe the requirements of the IRB are stringent enough and therefore, clinical research should be exempt from any new or additional requirements. The NPUAP also believes that access to encoded data should be excluded from any new requirements or restrictions applicable to information that identifies the patient. Only data sources or collections of samples that directly identify individuals should be subject to confidentiality protections. Finally, uniform national standards that preempt state laws concerning confidentiality are necessary.

The NPUAP thanks you for the opportunity to submit this written testimony. We would be happy to provide you with any additional information or answer any questions you may have.

Statement of Congressman Christopher Shays

Thank you Mr. Chairman and Members of the Committee for the opportunity to provide you with my thoughts on medical records confidentiality.

On September 11, Secretary Shalala testified that protecting the confidentiality of medical records is critical as our health system enters the 21st century. I couldn't agree more.

Under the Health Insurance Portability and Accountability Act, known as HIPAA or Kassebaum-Kennedy, Congress set a schedule for action on this issue. Should Congress fail to enact comprehensive legislation to protect the confidentiality of patients' medical records by August of next year, the Secretary will promulgate regulations by February 2000. I do not welcome the prospect that the Secretary will impose regulations—without Congressional debate or review—that could impact all facets of our health care system.

I want to recognize the efforts of Senators Bennett and Jeffords to move forward in this area. Their recognition that this is a serious problem has elevated the debate to a "must do" issue. Generally, the Senate has been driving the debate on legislation to protect the confidentiality of medical records. I am concerned, however, that the approach currently being devised by the Senate Labor Committee is overly burdensome. That is why I have been working on a different approach to spark discussion on this side of Capitol Hill. It is an important effort that I hope this subcommittee examines carefully.

Mr. Chairman, this is a complex problem that spans a broad spectrum of interests. In general, there are two opposing camps with very distinct and legitimate claims. One seeks to secure absolute privacy that would make it difficult, if not impossible, to coordinate the delivery of health services. The other seeks to protect the confidentiality of medical records and maintain largely untouched the current low standard of protections currently afforded to health information. I believe the solution lies somewhere in between.

Those who seek to secure absolute privacy in a health context are prescribing a disaster for our health delivery system. We need to balance competing interests, between a person's legitimate expectation of confidentiality and a business's need to know what it is paying for. In my judgment, the way to accomplish this is to leave the computer databases alone—and criminalize misuse of their data, recognizing there are both appropriate and inappropriate uses for medical information.

Unfortunately, there is no guiding legal principle in this area. Instead, there is a patchwork of state and federal law that protects people in some states with some diagnoses but not others. A strong, uniform law is necessary to preempt the quilt of state protections that treat medical records differently. Multi-state health plans that submit bills to clearinghouses who then forward claims to separate payors cannot operate through a maze of differing standards, regulations and restrictions.

The bill I intend to introduce next week, hopefully with the Chairman's support, will protect the confidentiality of medical records while protecting legitimate uses. The legislation will delineate the inappropriate uses of medical information—such as intentional or negligent disclosure, sale or commercial publication, or the use of

fraud, deceit or misrepresentation to access information. These prohibitions relate specifically to individually identifiable information. Use of anonymous information will not be affected, unless intentionally decoded.

In addition, my bill will allow patients to inspect, copy and, where appropriate, amend their medical records. Finally, the bill will impose strong criminal and civil penalties for inappropriate disclosures, and will preempt state law, creating a uniform system. Combined, these proposals should enhance the security of the patient medical record without jeopardizing advances in quality health care.

With current technology and future advances there are both real dangers and substantial opportunities with respect to protected health information. Absent strong, practical and workable standards, many will fall victim to those dangers and opportunities will be missed.

Innovative developments in the delivery of health services and technological advancements mean health information is both more important and more vulnerable. While we can all agree that sensitive information such as psychological evaluations and drug abuse counseling needs to be kept private, we also need to allow health plans and researchers to review health information to improve education and treatment.

It is my hope we can pass a national confidentiality law assuring patients' rights, while balancing the interests of payors and providers, data processors, law enforcement agencies, and researchers. Congress should pass legislation to secure the confidentiality of medical records, and it should be done this year.

Mr. Chairman, I appreciate the opportunity to share these views with you.